ESET Smart Security 4

Guia do usuário

(destina-se à versão 4.2 ou superior do produto)

Microsoft® Windows® 7 / Vista / XP / 2000 / 2003 / 2008

ESET Smart Security 4

Atendimento ao cliente mundial: www.eset.eu/support
Atendimento ao cliente da América do Norte: www.eset.com/support

REV.20100225-015

Conteúdo

1. ESET Smart Security 4

O ESET Smart Security 4 é o primeiro representante do novo foco de segurança de um computador realmente integrado. Ele utiliza a velocidade e a precisão do ESET NOD32 Antivírus, que é garantido pela versão mais recente do mecanismo de busca ThreatSense®, combinado com os módulos Firewall pessoal e Antispam. O resultado é um sistema inteligente que está constantemente em alerta contra ataques e softwares maliciosos que colocam em perigo o seu computador.

O ESET Smart Security não é um aglomerado de vários produtos em um pacote, como o que é oferecido por outros fornecedores. Ele é o resultado de um esforço de longo prazo para combinar a máxima proteção com o mínimo impacto do sistema. As tecnologias avançadas baseadas em inteligência artificial são capazes de eliminar proativamente a penetração dos vírus, spywares, cavalos de Troia, worms, adwares, rootkits e outros ataques provenientes da Internet, sem prejudicar o desempenho do sistema ou interromper o funcionamento do seu computador.

1.1 O que há de novo

A experiência em desenvolvimento de longo prazo de nossos especialistas é demonstrada por toda a nova arquitetura do ESET Smart Security, que garante máxima detecção com o mínimo de requisitos do sistema. Essa solução de segurança robusta contém módulos com diversas opções avançadas. A lista a seguir oferece uma breve visão geral desses módulos.

- **Antivírus e antispyware**

Esse módulo é construído sobre o mecanismo de rastreamento ThreatSense®, que foi usado pela primeira vez no premiado sistema NOD32 Antivírus. O ThreatSense® foi otimizado e melhorado com a nova arquitetura do ESET Smart Security.

Recurso	Descrição
Limpeza melhorada	O sistema antivírus agora limpa e exclui inteligentemente a maioria das ameaças detectadas, sem exigir a intervenção do usuário.
Modo de rastreamento em segundo plano	O rastreamento do computador pode ser iniciado em segundo plano sem diminuir o desempenho.
Arquivos de atualização menores	O processo de otimização central mantém o tamanho dos arquivos de atualização menores do que na versão 2.7. Também, a proteção dos arquivos de atualização contra danos foi melhorada.
Proteção de cliente de email popular	Agora é possível rastrear os emails recebidos não somente no Microsoft Outlook, mas também no Outlook Express, no Windows Mail, no Windows Live Mail e no Mozilla Thunderbird.
Outras melhorias secundárias	– Acesso direto aos sistemas de arquivos para alta velocidade e resultado. – Acesso bloqueado aos arquivos infectados. – Otimização para o Windows Security Center, incluindo o Vista.

- **Firewall pessoal**

O Firewall pessoal monitora o tráfego entre um computador protegido e os demais computadores na rede. O Firewall pessoal da ESET contém as funções avançadas listadas a seguir.

Recurso	Descrição
Perfis	Perfis são uma ferramenta para controlar o comportamento do Firewall pessoal do ESET Smart Security. Vários perfis que podem ter diferentes regras atribuídas a eles permitem que os usuários alterem com facilidade o comportamento do firewall pessoal.
Autenticação da zona	Permite que os usuários identifiquem a rede à qual se conectam e definam uma ação (por exemplo, alternar o perfil do firewall e bloquear a comunicação com a zona) com base nessas informações.
Verificação da comunicação da rede na camada inferior	A verificação da comunicação da rede na Camada do Data Link permite que o Firewall pessoal da ESET se sobreponha a diversos ataques que, de outra forma, não seriam detectados.
Suporte IPv6	O Firewall pessoal da ESET exibe os endereços IPv6 e permite que os usuários criem regras para eles.
Monitoramento de arquivos executáveis	Monitoramento das alterações em arquivos executáveis, a fim de impedir a infecção. É possível permitir uma modificação do arquivo de aplicativos assinados (confiáveis).
Rastreamento de arquivos integrado com o HTTP(s) e o POP3(s)	Rastreamento integrado de arquivos dos protocolos de aplicativo HTTP(s) e POP3(s). Os usuários estão protegidos ao navegar na Internet ou fazer o download de emails.
Sistema de detecção de invasão	Capacidade de reconhecer o caractere da comunicação da rede e de diversos tipos de ataques à rede com uma opção de banir automaticamente tais comunicações.
Modo interativo, com base em políticas, de aprendizagem e automático com exceções	Os usuários podem selecionar se as ações do firewall pessoal serão executadas automaticamente ou se desejam estabelecer regras interativamente. A comunicação com base em políticas é administrada de acordo com as regras predefinidas pelo usuário ou pelo administrador da rede. O Modo de aprendizagem cria e salva automaticamente as regras e é adequado para a configuração inicial do firewall.
Substitui o Firewall integrado do Windows	Substitui o Firewall integrado do Windows e interage com o Windows Security Center para monitorar o status de segurança. A instalação do ESET Smart Security desativa o firewall do Windows por padrão.

- **Antispam**

O ESET Antispam filtra os emails não solicitados e portanto aumenta a segurança e o conforto da comunicação eletrônica.

Recurso	Descrição
Pontuação dos emails recebidos	Todos os emails recebidos são classificados com uma pontuação de 0 (uma mensagem que não é spam) a 100 (uma mensagem spam) e filtrados de acordo para a pasta Lixo Eletrônico ou para uma pasta personalizada criada pelo usuário. O rastreamento paralelo de emails recebidos é possível.
Suporta diversas técnicas de rastreamento	– Análise Bayes. – Rastreamento baseado em regras. – Verificação do banco de dados de impressão digital global.
Integração total aos clientes de email	A proteção antispam está disponível para os usuários de clientes do Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.
A seleção de spam manual está disponível	Opção de selecionar/desmarcar manualmente emails como spam.

- **Outros**

Recurso	Descrição
ESET SysRescue	O ESET SysRescue permite que o usuário crie um CD/DVD/USB inicializável que contenha o ESET Smart Security, que é capaz de executar independentemente do sistema operacional. É mais adequado para livrar o sistema de ameaças difíceis de serem removidas.
ESET SysInspector	ESET SysInspector, um aplicativo que inspeciona completamente o seu computador, agora está integrado diretamente no ESET Smart Security. Se você entrar em contato com o Serviço de atendimento ao cliente utilizando a opção Ajuda e suporte > Solicitação de suporte ao Atendimento ao cliente (recomendado), é possível optar por incluir um instantâneo do status do ESET SysInspector do computador.
Proteção de documentos	O recurso Proteção de documentos serve para rastrear os documentos do Microsoft Office antes de eles serem abertos e os arquivos obtidos por download automaticamente pelo Internet Explorer, como, por exemplo, elementos do Microsoft ActiveX.
Autodefesa	A tecnologia Autodefesa protege os componentes do ESET Smart Security contra tentativas de desativação.
Interface do usuário	A interface do usuário agora é capaz de trabalhar em modo não gráfico, o que permite o controle de teclado do ESET Smart Security. O aumento da compatibilidade com o aplicativo de leitura de tela permite que as pessoas portadoras de deficiências visuais controlem o programa com mais eficiência.

1.2 Requisitos do sistema

Para uma operação sem interrupções do ESET Smart Security e do ESET Smart Security Business Edition, o sistema deve atender aos seguintes requisitos de hardware e de software:

ESET Smart Security:

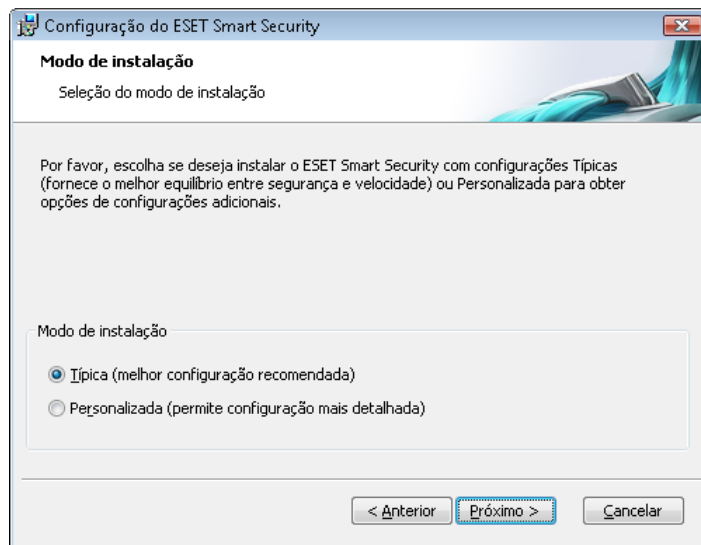
Windows 2000, XP	400 MHz 32 bits / 64 bits (x86 / x64) 128 MB RAM de memória do sistema 130 MB de espaço disponível Super VGA (800 × 600)
Windows 7, Vista	1 GHz 32 bits / 64 bits (x86 / x64) 512 MB RAM de memória do sistema 130 MB de espaço disponível Super VGA (800 × 600)

ESET Smart Security Business Edition:

Windows 2000, 2000 Server, XP, 2003 Server	400 MHz 32 bits / 64 bits (x86 / x64) 128 MB RAM de memória do sistema 130 MB de espaço disponível Super VGA (800 × 600)
Windows 7, Vista, Windows Server 2008	1 GHz 32 bits / 64 bits (x86 / x64) 512 MB RAM de memória do sistema 130 MB de espaço disponível Super VGA (800 × 600)

2. Instalação

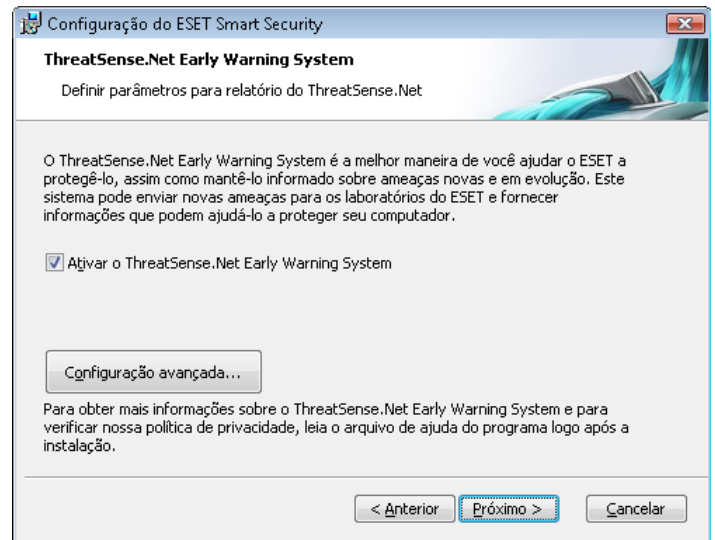
Após a compra, o instalador do ESET Smart Security pode ser obtido através de download no site da ESET. Ele é fornecido como um pacote ess_nt**_***.msi (ESET Smart Security) ou essbe_nt**_***.msi (ESET Smart Security Business Edition). Inicie o instalador e o assistente de instalação o guiará pela configuração básica. Há dois tipos de instalação disponíveis com diferentes níveis de detalhes de configuração:

1. Instalação típica
2. Instalação personalizada

2.1 Instalação típica

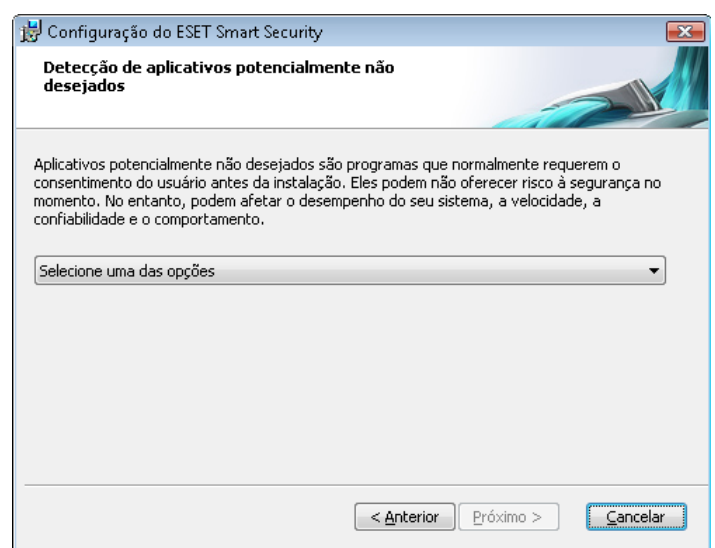
A Instalação típica é recomendada para usuários que desejam instalar o ESET Smart Security com as configurações padrão. As configurações padrão do programa fornecem o nível máximo de proteção, um fato apreciado pelos usuários que não desejam definir configurações detalhadas.

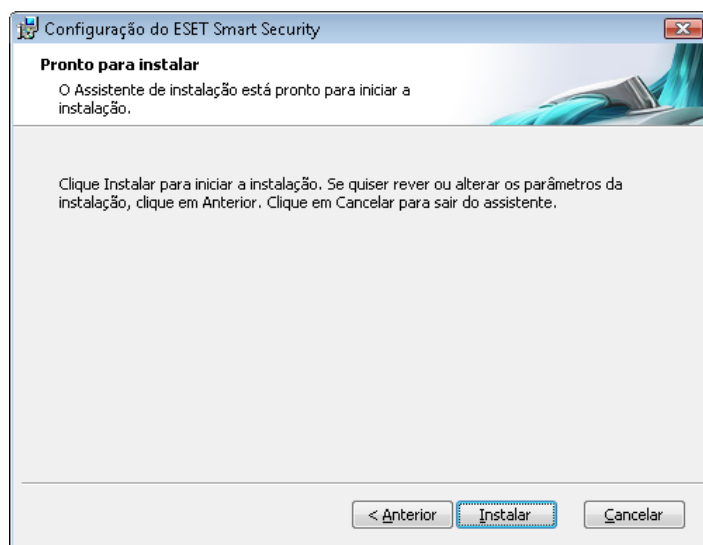
A primeira e muito importante etapa é digitar o nome de usuário e a senha para atualização automática do programa. Essa etapa tem um papel significativo no fornecimento de proteção constante ao sistema.

Digite o seu **Nome de usuário** e **Senha**, ou seja, os dados de autenticação recebidos após a compra ou o registro do produto, nos campos correspondentes. Se você não tiver o Nome de usuário e a Senha disponíveis no momento, selecione a opção **Configurar parâmetros de atualização mais tarde**. Os dados de autenticação podem ser inseridos posteriormente a qualquer momento, diretamente no programa.

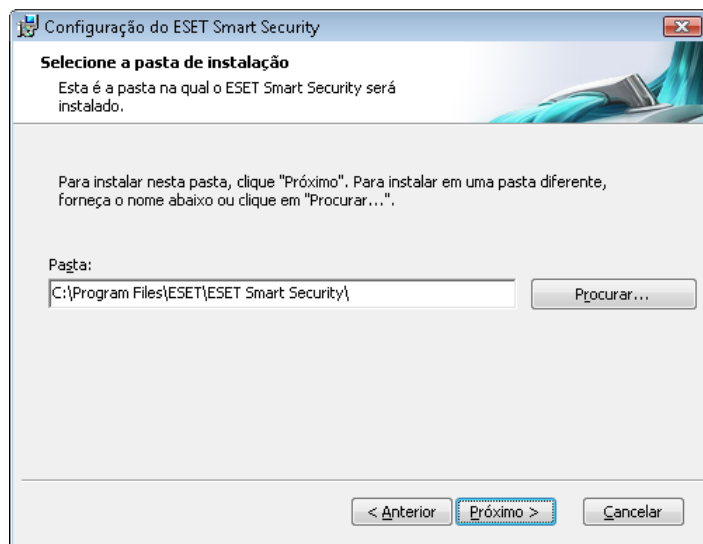
A próxima etapa da instalação é a configuração do ThreatSense.Net Early Warning System. O ThreatSense.Net Early Warning System ajuda a garantir que a ESET seja informada contínua e imediatamente sobre novas ameaças para proteger rapidamente seus clientes. O sistema permite o envio de novas ameaças para o laboratório de vírus da ESET, onde elas são analisadas, processadas e adicionadas aos bancos de dados de assinatura de vírus.

Por padrão, a caixa de seleção **Ativar o ThreatSense.Net Early Warning System** está selecionada, o que ativará esse recurso. Clique em **Configuração avançada...** para modificar as configurações detalhadas para o envio de arquivos suspeitos.

A próxima etapa do processo de instalação é a configuração da **Detecção de aplicativos potencialmente indesejados**. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar negativamente o comportamento do sistema operacional.

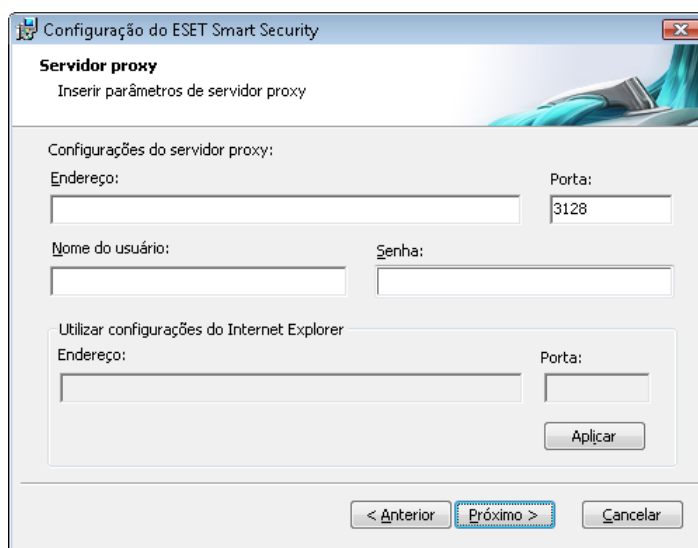
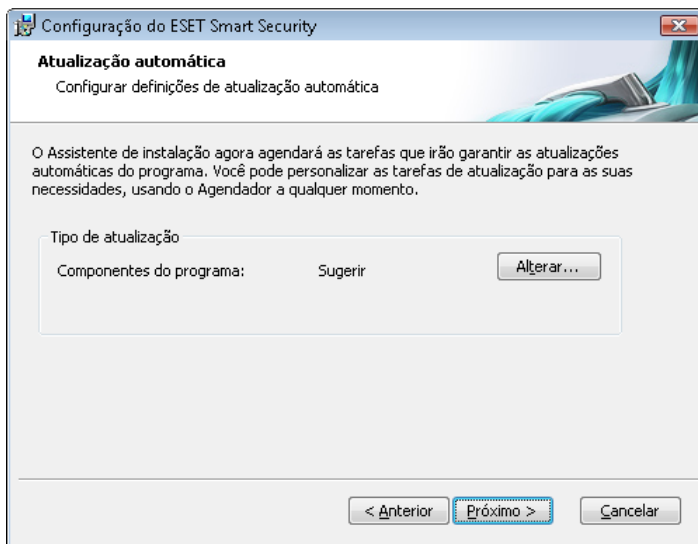
Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento.

Selecione a opção **Ativar detecção de aplicativos potencialmente indesejados** para permitir que o ESET Smart Security detecte este tipo de ameaça (recomendável).

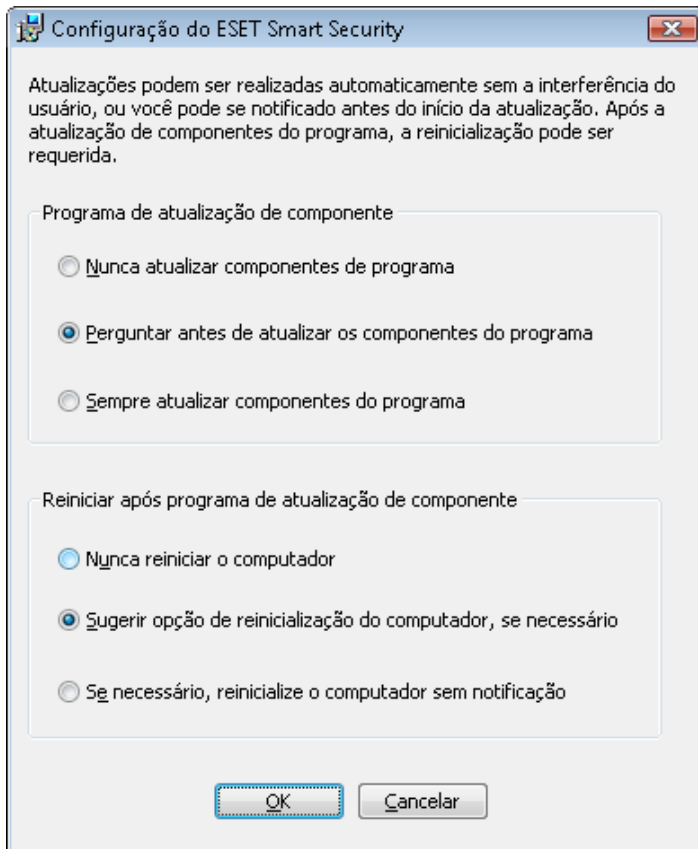
A última etapa no modo de Instalação típica é a confirmação da instalação clicando no botão **Instalar**.

2.2 Instalação personalizada

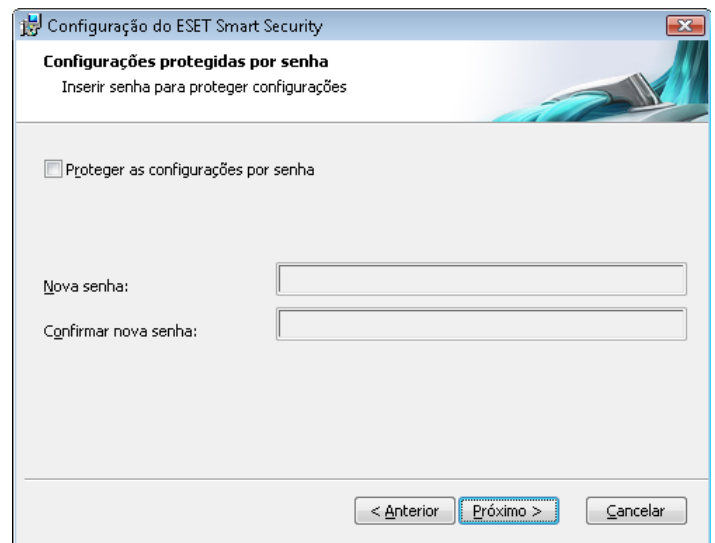
A Instalação **personalizada** é destinada a usuários experientes em ajuste de programas e que desejam modificar configurações avançadas durante a instalação.

A primeira etapa é selecionar o local de destino para a instalação. Por padrão, o programa é instalado em C:\Arquivos de Programas\ESET\ESET Smart Security\. Clique em **Procurar...** para alterar esse local (não recomendável).

Em seguida, **Digite seu nome de usuário e senha**. Essa etapa é igual à da Instalação típica (consulte a página 5).

Depois de digitar o seu Nome de usuário e Senha, clique em **Avançar** para **Configurar sua conexão com a Internet**.

Se utilizar um servidor proxy, ele deverá ser configurado corretamente para que as atualizações de assinatura de vírus funcionem adequadamente. Se você não souber se utiliza ou não um servidor proxy para se conectar à Internet, mantenha a configuração padrão **Não tenho certeza se a minha conexão com a Internet usa um servidor proxy. Utilize as mesmas configurações do Internet Explorer** e clique em **Avançar**. Se não utilizar um servidor proxy, selecione a opção correspondente.

Para definir as configurações do servidor proxy, selecione **Eu utilizo um servidor proxy** e clique em **Avançar**. Digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço.** No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Caso o servidor proxy exija autenticação, um nome de usuário e uma senha válidos devem ser digitados, o que concede acesso ao servidor proxy. As configurações do servidor proxy também podem ser copiadas do Internet Explorer se desejar. Para fazer isso, clique em **Aplicar** e confirme a seleção.

Clique em **Avançar** para prosseguir na janela **Configurar definições de atualização automática**. Essa etapa permite especificar como as atualizações automáticas dos componentes do programa serão tratadas no sistema. Clique em **Alterar...** para acessar as configurações avançadas.

Se não desejar atualizar os componentes do programa, selecione **Nunca atualizar componentes do programa**. A ativação da opção **Perguntar antes de fazer download dos componentes do programa** exibirá uma janela de confirmação para fazer download dos componentes do programa. Para ativar a atualização automática dos componentes do programa sem avisar, selecione a opção **Realizar a atualização dos componentes do programa, se disponível**.

OBSERVAÇÃO: Após uma atualização dos componentes do programa, uma reinicialização é normalmente necessária. A configuração recomendada é: **Se necessário, reinicie o computador sem notificação**.

A próxima etapa da instalação é Digitar uma senha para proteger os parâmetros do programa. Escolha uma senha com a qual deseja proteger o programa. Digite a senha novamente para confirmar.

As etapas **Configuração do ThreatSense.Net Early Warning System** e **Detecção de aplicativos potencialmente indesejados** são as mesmas de uma Instalação típica e não são mostradas aqui (consulte a página 6).

A última etapa no modo Personalizado é selecionar o modo de filtragem do Firewall pessoal da ESET. Há cinco modos disponíveis:

- Automático
- Modo automático com exceções (regras definidas pelo usuário)
- Interativo
- Com base em políticas
- De aprendizagem

O Modo **automático** é recomendado para a maioria dos usuários. Todas as conexões de saída padrão são ativadas (automaticamente analisadas utilizando as configurações padrão), e as conexões de entrada não solicitadas são bloqueadas automaticamente.

Modo automático com exceções (regras definidas pelo usuário). Além do modo automático, ele permite adicionar regras personalizadas.

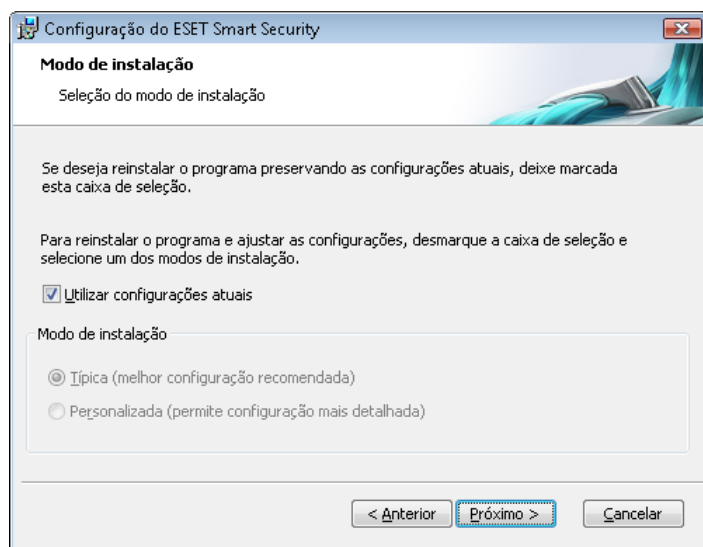
O Modo **interativo** é adequado para usuários avançados. As comunicações são tratadas por regras definidas pelo usuário. Se não houver nenhuma regra definida para uma comunicação, o programa pergunta ao usuário se ele permite ou nega a comunicação.

O Modo **com base em políticas** avalia a comunicação com base em regras predefinidas criadas pelo administrador. Se não houver nenhuma regra disponível, a conexão é bloqueada automaticamente, e o usuário não vê nenhuma mensagem de aviso. Recomendamos que selecione somente o Modo com base em políticas se for um administrador que pretenda configurar a comunicação de rede.

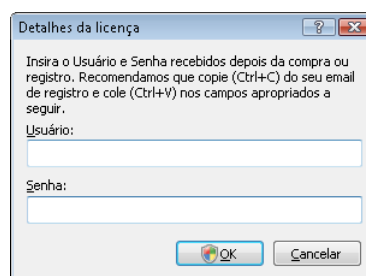
Modo de aprendizagem – Cria e salva automaticamente as regras e é adequado para a configuração inicial do firewall pessoal. Nenhuma interação com o usuário é exigida, porque o ESET Smart Security salva as regras de acordo com os parâmetros predefinidos. O Modo de aprendizagem não é seguro e deve ser usado apenas até que todas as regras para as comunicações exigidas tenham sido criadas.

A última etapa mostra uma janela que exige o seu consentimento para instalar.

2.3 Uso de configurações originais

Se você reinstalar o ESET Smart Security, a opção **Utilizar configurações atuais** será exibida. Selecione essa opção para transferir parâmetros de configuração da instalação original para uma nova instalação.

2.4 Digitação de nome de usuário e senha

Para obter a funcionalidade ideal, é importante que o programa seja atualizado automaticamente. Isso somente será possível se o nome de usuário e a senha corretos forem digitados na configuração da atualização.

Se você não digitou o seu nome de usuário e a senha durante a instalação, poderá digitá-los agora. Na janela principal do programa, clique na opção **Atualizar** e, em seguida, na opção **Configuração de nome de usuário e senha...** Digite os dados recebidos com a licença do produto na janela **Detalhes da licença**.

2.5 Rastreamento sob demanda do computador

Após a instalação do ESET Smart Security, um rastreamento no computador para verificar a presença de código malicioso deverá ser executado. Para iniciar o rastreamento rapidamente, selecione **Rastrear o computador** no menu principal e selecione **Rastreamento padrão** na janela principal do programa. Para obter mais informações sobre o recurso Rastreamento do computador, consulte o capítulo "Rastreamento do computador".

3. Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET Smart Security e de suas configurações básicas.

3.1 Introdução ao design da interface do usuário – modos

A janela principal do ESET Smart Security é dividida em duas seções principais. A coluna à esquerda fornece acesso ao menu principal de fácil utilização. A janela principal do programa à direita serve principalmente para exibir informações correspondentes à opção selecionada no menu principal.

A seguir, há uma descrição dos botões dentro do menu principal:

Status da proteção – Em um formato de fácil utilização, ele fornece informações sobre o status de proteção do ESET Smart Security. Se o modo Avançado estiver ativado, o status de todos os módulos de proteção será exibido. Clique em um módulo para exibir o seu status atual.

Rastrear o computador – Essa opção permite que o usuário configure e inicie o rastreamento sob demanda do computador.

Atualizar – Selecione essa opção para acessar o módulo de atualização que gerencia atualizações para o banco de dados de assinatura de vírus.

Configuração – Selecione essa opção para ajustar o nível de segurança do seu computador. Se o Modo avançado estiver ativado, os submenus Proteção antivírus e antispyware, Firewall pessoal e o Módulo antispam serão exibidos.

Ferramentas – Essa opção está disponível somente no modo Avançado. Fornece acesso a Relatórios, Quarentena e Agenda.

Ajuda e suporte – Selecione essa opção para acessar os arquivos da ajuda, a base de conhecimento da ESET, o site da ESET na Web e acessar uma solicitação de suporte ao Atendimento ao cliente.

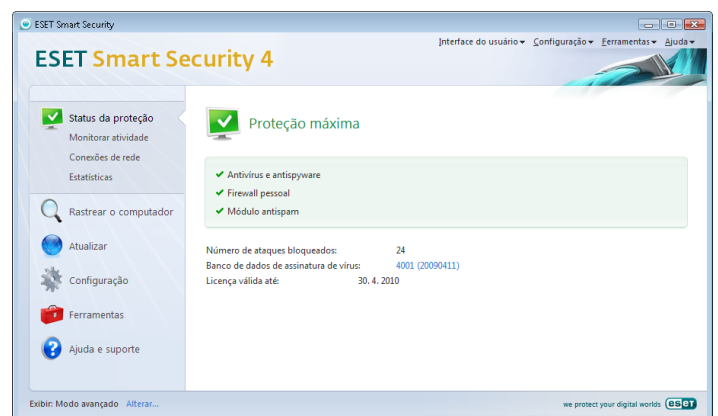
A interface do usuário do ESET Smart Security permite que os usuários alternem entre os modos Padrão e Avançado. Para alternar entre os modos, consulte o link **Exibir** localizado no canto inferior esquerdo da janela principal do ESET Smart Security. Clique nesse botão para selecionar o modo de exibição desejado.

O Modo padrão fornece acesso aos recursos necessários para operações comuns. Ele não exibe opções avançadas.

A alternância para o modo Avançado adiciona a opção **Ferramentas** ao menu principal. A opção Ferramentas permite que o usuário acesse a Agenda, a Quarentena ou exiba os Relatórios do ESET Smart Security.

OBSERVAÇÃO: Todas as instruções restantes deste guia ocorrerão no modo Avançado.

3.1.1 Verificação do funcionamento do sistema

Para exibir o **Status da proteção**, clique nessa opção no topo do menu principal. Um resumo de status sobre o funcionamento do ESET Smart Security é exibido no lado direito da janela, e um submenu com três itens aparece: **Antivírus e antispyware**, **Firewall pessoal** e **Módulo antispam**. Selecione qualquer um deles para exibir informações mais detalhadas sobre um determinado módulo de proteção.

Se os módulos ativados estiverem funcionando adequadamente, uma marca verde será atribuída a eles. Caso contrário, um ponto de exclamação vermelho ou um ícone de notificação laranja será exibido, e informações adicionais sobre o módulo serão mostradas na parte superior da janela. Uma solução sugerida para corrigir o módulo também é exibida. Para alterar o status dos módulos individuais, clique em **Configuração** no menu principal e clique no módulo desejado.

3.1.2 O que fazer se o programa não funciona adequadamente

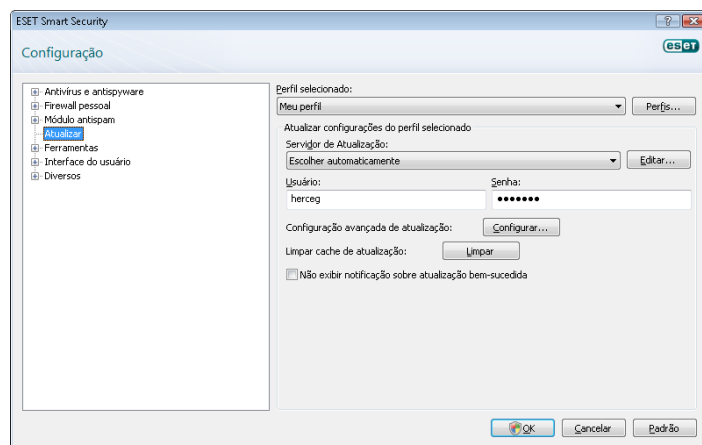
Se o ESET Smart Security detectar um problema em qualquer um dos seus módulos de proteção, ele será relatado na janela **Status da proteção**. Uma sugestão para a solução do problema também é fornecida aqui.

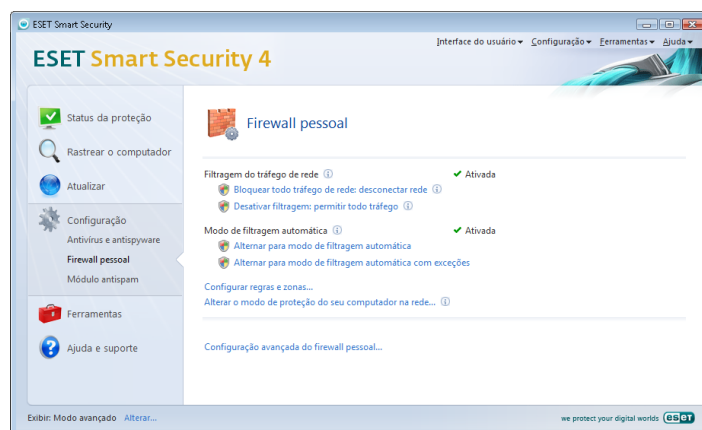
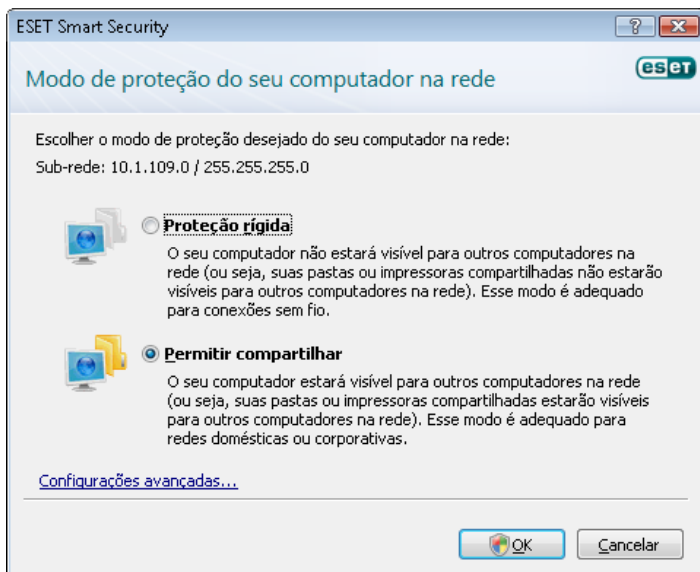
Se não for possível solucionar um problema utilizando a lista exibida de problemas conhecidos e soluções, clique em **Ajuda e suporte** para acessar os arquivos de ajuda ou procure a Base de conhecimento. Se uma solução ainda não puder ser encontrada, você pode enviar uma solicitação de suporte ao Atendimento ao cliente da ESET. Com base nessas informações fornecidas, nossos especialistas podem responder rapidamente às suas questões e aconselhá-lo com mais eficiência sobre o problema.

3.2 Configuração da atualização

A atualização do banco de dados de assinatura de vírus e a atualização dos componentes do programa são partes importantes no fornecimento de proteção completa contra códigos maliciosos. Dê atenção especial à configuração e operação delas. No menu principal, selecione **Atualizar** e clique em **Atualizar banco de dados de assinatura de vírus** na janela principal do programa para verificar instantaneamente quanto à disponibilidade de uma atualização de banco de dados mais recente. **Configuração de nome de usuário e senha...** exibe uma caixa de diálogo em que o Nome de usuário e Senha, recebidos no momento da compra, devem ser digitados.

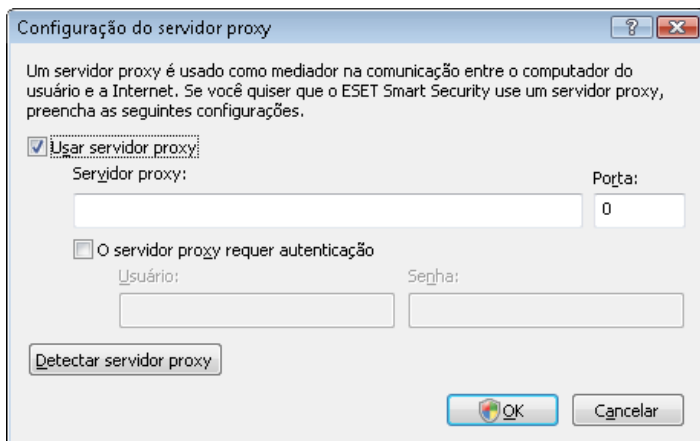
Se o Nome de usuário e a Senha foram digitados durante a instalação do ESET Smart Security, você não será solicitado a fornecê-los neste ponto.

A janela **Configuração avançada** (pressione F5 para acessar) contém outras opções de atualização detalhadas. O menu suspenso **Atualizar servidor:** deve ser configurado como **Escolher automaticamente**. Para configurar as opções de atualização avançadas, como o modo de atualização, o acesso ao servidor proxy, acessando as atualizações em um servidor local e criando cópias de assinatura de vírus (ESET Smart Security Business Edition), clique no botão **Configuração...**

3.3 Configuração de zona confiável

A configuração de uma Zona confiável é uma etapa importante na proteção do seu computador em um ambiente de rede. É possível permitir que outros usuários acessem o seu computador configurando a Zona confiável para permitir o compartilhamento. Clique em **Configuração > Firewall pessoal >Alterar o modo de proteção do seu computador na rede...** Uma janela será exibida permitindo que você defina as configurações do modo de proteção do computador na zona/rede real.

A detecção da Zona confiável é executada após a instalação do ESET Smart Security e a qualquer hora que o computador estiver conectado a uma nova rede. Portanto, não há necessidade de definir a Zona confiável na maioria dos casos. Por padrão, há uma janela de diálogo exibida na detecção de uma nova zona que permite que você configure o nível de proteção dessa zona.

Aviso! Uma configuração incorreta da zona confiável pode representar um risco de segurança para o seu computador.

OBSERVAÇÃO: Por padrão, as estações de trabalho de uma Zona confiável têm acesso garantido a arquivos e impressoras compartilhados, a comunicação RPC de entrada é ativada e o compartilhamento da área de trabalho remota também está disponível.

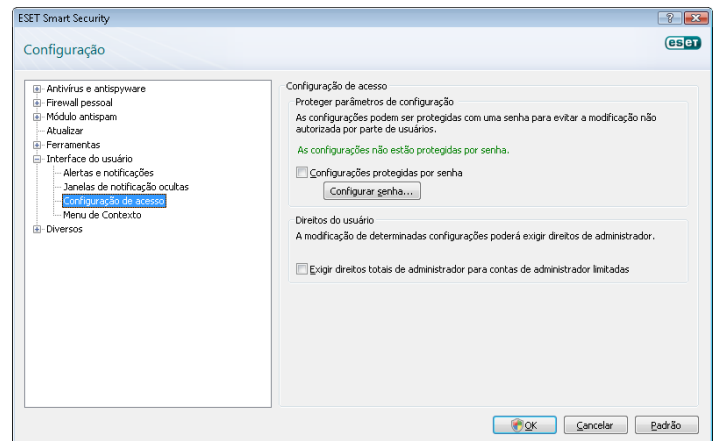
3.4 Configuração do servidor proxy

Se utilizar um servidor proxy para mediar a conexão com a Internet em um sistema utilizando o ESET Smart Security, ele deve ser especificado na Configuração avançada (F5). Para acessar a janela de configuração do **Servidor proxy**, clique em **Diversos > Servidor proxy**, na árvore Configuração avançada. Marque a caixa de seleção **Usar servidor proxy** e digite o endereço IP e a porta do servidor proxy, junto com os dados de autenticação.

Se essas informações não estiverem disponíveis, é possível tentar detectar automaticamente as configurações do servidor proxy para o ESET Smart Security clicando no botão **Detectar servidor proxy**.

OBSERVAÇÃO: As opções de servidor proxy para diferentes perfis de atualização podem variar. Nesse caso, configure o servidor proxy na configuração avançada de atualização.

3.5 Proteção de configurações

As Configurações do ESET Smart Security podem ser muito importantes na perspectiva da política de segurança de sua organização. Modificações não autorizadas podem potencialmente pôr em risco a estabilidade e a proteção do seu sistema. Para proteger os parâmetros da configuração por senha, inicie no menu principal e clique em **Configuração > Entrar na configuração avançada... > Interface do usuário > Proteção de configurações** e clique no botão **Inserir senha...**

Digite uma senha, confirme-a digitando-a novamente e clique em **OK**. Essa senha será exigida para as modificações futuras nas configurações do ESET Smart Security.

4. Trabalho com o ESET Smart Security

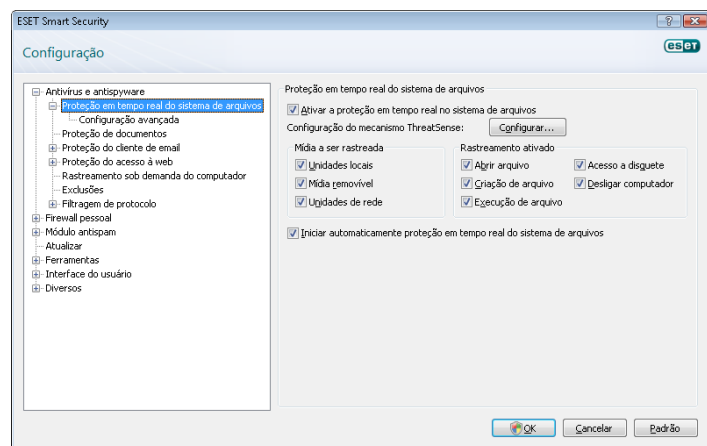
4.1 Proteção antivírus e antispyware

A proteção antivírus protege contra ataques de sistemas maliciosos ao controlar arquivos, emails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la primeiro bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena.

4.1.1 Proteção em tempo real do sistema de arquivos

A proteção em tempo real do sistema de arquivos controla todos os eventos do sistema relacionados a antivírus. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção do sistema em tempo real é ativada na inicialização do sistema.

4.1.1.1 Configuração de controle

A proteção de sistema de arquivos em tempo real verifica todos os tipos de mídia e é acionada por vários eventos. O controle utiliza os métodos de detecção da tecnologia ThreatSense (conforme descrito em Configuração de parâmetros do mecanismo ThreatSense).
O comportamento do controle em arquivos recém-criados e em arquivos existentes pode variar. Em arquivos recém-criados, é possível aplicar um nível mais profundo de controle.

4.1.1.1.1 Mídia a ser rastreada

Por padrão, todos os tipos de mídia são rastreados quanto a ameaças potenciais.

Unidades locais – Controla todas as unidades de disco rígido do sistema

Mídia removível – Disquetes, dispositivos de armazenamento USB, etc.

Unidades de rede – Rastreia todas as unidades mapeadas

Recomendamos manter as configurações padrão e modificá-las somente em casos específicos, como quando o rastreamento de determinada mídia tornar muito lenta a transferência de dados.

4.1.1.1.2 Rastreamento ativado (Rastreamento acionado por evento)

Por padrão, todos os arquivos são verificados na abertura, execução ou criação. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador.

A opção **Acesso a disquete** fornece o controle do setor de inicialização do disquete quando essa unidade for acessada. A opção **Desligar computador** fornece o controle dos setores de inicialização do disco rígido durante o desligamento do computador. Embora os vírus de inicialização sejam raros atualmente, recomendamos deixar essas opções ativadas, pois sempre há a possibilidade de infecção por um vírus de inicialização de origem alternativa.

4.1.1.1.3 Parâmetros adicionais do ThreatSense para arquivos criados e modificados recentemente

A probabilidade de infecção em arquivos recém-criados ou recém-modificados é comparativamente mais alta que nos arquivos já existentes. É por isso que o programa verifica esses arquivos com mais parâmetros de rastreamento. Junto com os métodos de rastreamento baseados em assinaturas comuns, é usada heurística avançada, que aumenta enormemente os índices de detecção. Além dos arquivos recém-criados, o rastreamento também é feito nos arquivos de extração automática (SFX) e nos empacotadores em tempo de execução (arquivos executáveis compactados internamente).
Por padrão, os arquivos compactados são rastreados até o décimo nível de aninhamento e são verificados, independentemente do tamanho real deles. Desmarque a opção ***Configuração padrão de rastreamento em arquivos compactados*** para modificar as configurações de rastreamento em arquivos compactados.

4.1.1.1.4 Configuração avançada

Para fornecer baixo impacto no sistema ao usar a proteção em tempo real, os arquivos já verificados não serão rastreados repetidas vezes (a menos que tenham sido modificados). Os arquivos são verificados novamente logo após cada atualização do banco de dados de assinaturas de vírus. Esse comportamento é configurado utilizando a opção **Rastreamento otimizado**. Se esse recurso for desativado, todos os arquivos serão rastreados sempre que forem acessados.

Por padrão, a proteção em tempo real é iniciada no momento da inicialização do sistema operacional, fornecendo rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outro rastreador em tempo real), a proteção em tempo real poderá ser interrompida, desativando a opção **Inicialização automática da proteção em tempo real do sistema de arquivos**.

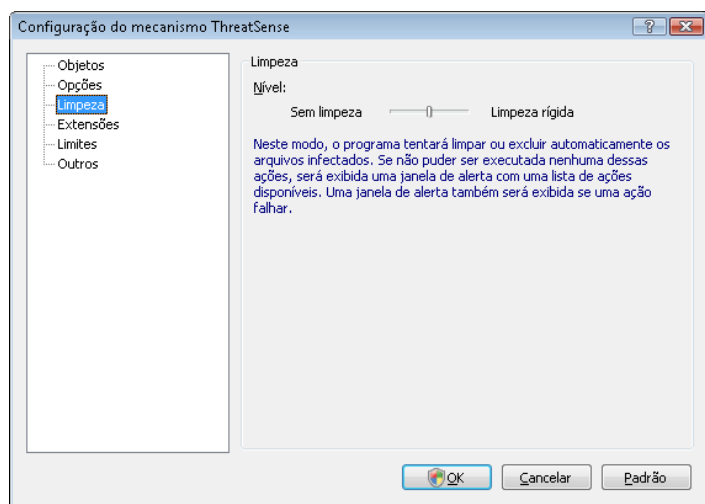
Por padrão, a heurística avançada não é utilizada quando os arquivos são executados. Entretanto, em alguns casos, pode ser que você queira ativar essa opção (marcando a opção **Heurística avançada na execução de arquivos**). Observe que a heurística avançada pode tornar mais lenta a execução de alguns programas devido ao aumento dos requisitos do sistema.

4.1.1.2 Níveis de limpeza

A proteção em tempo real possui três níveis de limpeza (para acessar, clique no botão **Configuração...** na seção **Proteção em tempo real do sistema de arquivos** e, em seguida, clique na ramificação **Limpeza**).

- O primeiro nível exibe uma janela de alerta com as opções disponíveis para cada ameaça encontrada. O usuário precisa escolher uma ação para cada ameaça individualmente. Esse nível é destinado aos usuários mais avançados que sabem quais etapas realizar no caso de uma ameaça.

- O nível padrão escolhe e executa automaticamente uma ação predefinida (dependendo do tipo de ameaça). A detecção e a exclusão de um arquivo infectado são assinaladas por uma mensagem de informação localizada no canto inferior direito da tela. Entretanto, uma ação automática não é realizada se a ameaça estiver localizada dentro de um arquivo compactado que também contenha arquivos limpos, e não será realizada em objetos para os quais não haja ação predefinida.

- O terceiro nível é o mais "agressivo" – todos os objetos infectados são limpos. Uma vez que esse nível poderia potencialmente resultar em perda de arquivos válidos, recomendamos que seja usado somente em situações específicas.

4.1.1.3 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Portanto, seja cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos. Por exemplo, se houver um conflito com um determinado aplicativo ou rastreador em tempo real de outro programa antivírus.

Após a instalação do ESET Smart Security, todas as configurações serão otimizadas para fornecer o nível máximo de segurança do sistema para usuários. Para restaurar as configurações padrão, clique no botão **Padrão** localizado na parte inferior direita da janela **Proteção em tempo real do sistema de arquivos** (**Configuração avançada > Antivírus e antispyware > Proteção em tempo real do sistema de arquivos**).

4.1.1.4 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.org. Esse arquivo de teste é especial, inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus. O arquivo eicar.com está disponível para download no endereço http://www.eicar.org/download/eicar.com.

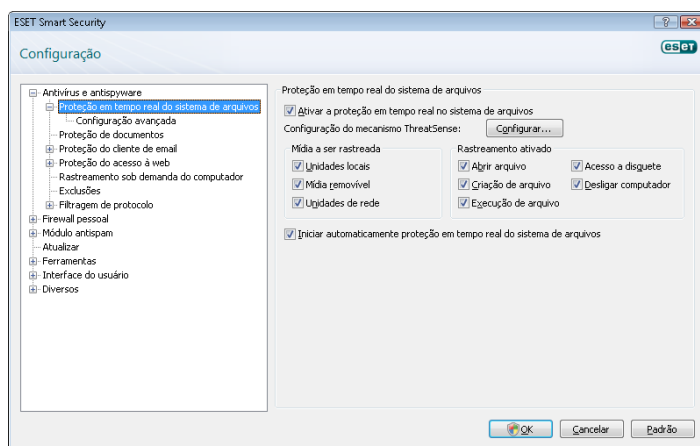
OBSERVAÇÃO: Antes de realizar um rastreamento da proteção de tempo real, é preciso desativar o firewall. Se o firewall estiver ativado, ele detectará e impedirá o download do arquivo de teste.

4.1.1.5 O que fazer se a proteção em tempo real não funcionar

No capítulo seguinte, descrevemos situações problemáticas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada

Se a proteção em tempo real foi inadvertidamente desativada por um usuário, é preciso reativá-la. Para reativar a proteção em tempo real, navegue até **Configuração > Antivírus e antispyware** e clique em **Ativar** na seção **Proteção em tempo real do sistema de arquivos** da janela principal do programa.

Se a proteção em tempo real não for ativada na inicialização do sistema, isso provavelmente será devido à desativação da opção **Inicialização automáticada proteção em tempo real do sistema de arquivos**. Para ativar essa opção, navegue até **Configuração Avançada** (F5) e clique em **Proteção do sistema de arquivos em tempo real**, na árvore Configuração avançada. Na seção **Configuração avançada** na parte inferior da janela, verifique se a caixa de seleção **Inicialização automática da proteção do sistema de arquivos em tempo real** está marcada.

Se a proteção em tempo real não detectar nem limpar ameaças

Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema.

Proteção em tempo real não é iniciada

Se a proteção em tempo real não for ativada na inicialização do sistema (e a opção **Inicialização automática da proteção em tempo real do sistema de arquivos** estiver ativada), isso pode ser devido a conflitos com outros programas. Nesse caso, consulte os especialistas do Serviço ao Cliente da ESET.

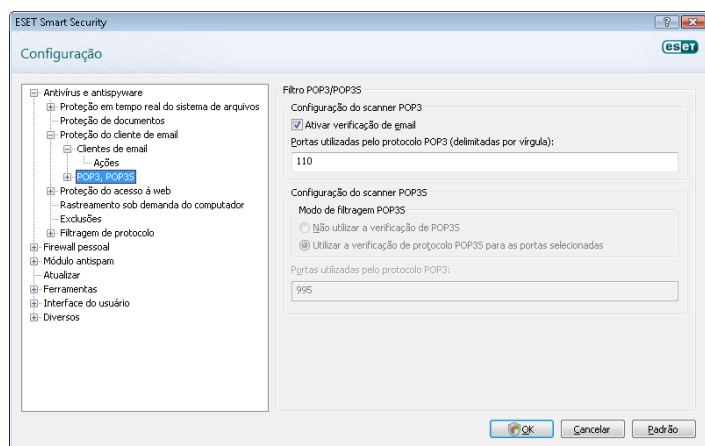
4.1.2 Proteção de cliente de email

A proteção de email fornece controle da comunicação por email recebida via protocolo POP3. Com o programa plug-in do Microsoft Outlook, o ESET Smart Security permite controlar todas as comunicações vindas do cliente de email (POP3, MAPI, IMAP, HTTP). Ao verificar mensagens de entrada, o programa usa todos os métodos de rastreamento avançado fornecidos pelo mecanismo de rastreamento ThreatSense. Isso significa que a detecção de programas maliciosos é realizada até mesmo antes de os mesmos serem comparados com o banco de dados de assinaturas de vírus. O rastreamento das comunicações via protocolo POP3 é independente do cliente de email utilizado.

4.1.2.1 Verificação de POP3

O protocolo POP3 é o protocolo mais amplamente utilizado para receber mensagens em um aplicativo de cliente de email. O ESET Smart Security fornece proteção a esse protocolo independentemente do cliente de email usado.

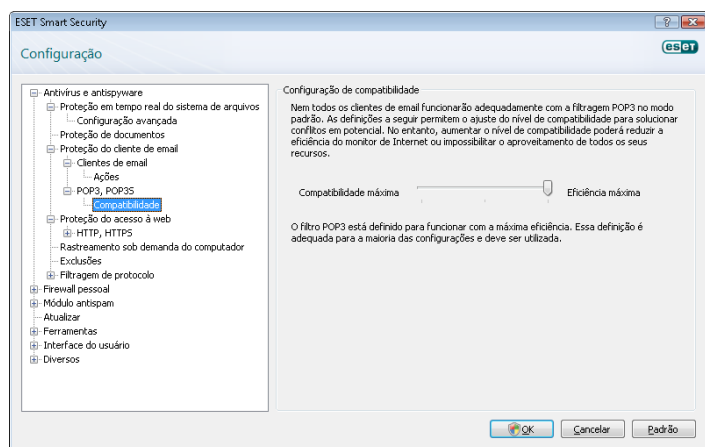
O módulo que permite esse controle é automaticamente ativado no momento da inicialização do sistema operacional e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado – a verificação de POP3 é feita automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os números das portas devem ser delimitados por vírgula.

A comunicação codificada não é controlada.

4.1.2.1.1 Compatibilidade

Alguns programas de email podem apresentar problemas com a filtragem POP3 (por exemplo, ao receber mensagens com uma conexão lenta de Internet, devido à verificação, pode ocorrer desativação por ultrapassar o limite de tempo). Nesse caso, tente modificar a maneira como é feito o controle. A redução do nível de controle pode melhorar a velocidade do processo de limpeza. Para ajustar o nível de controle da filtragem POP3, navegue até **Antivírus e antispyware > Proteção de email > POP3 > Compatibilidade**.

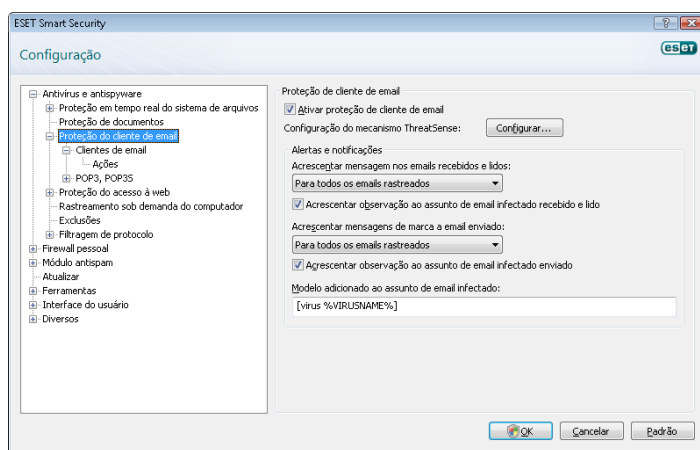
Se **Eficiência máxima** estiver ativada, as ameaças serão removidas das mensagens infectadas e as informações sobre a ameaça serão inseridas na frente do assunto original do email (as opções **Excluir** ou **Limpar** precisam estar ativadas ou o nível de limpeza **Rígida** ou **Padrão** precisa estar ativado).

Compatibilidade média modifica a maneira como as mensagens são recebidas. As mensagens são gradualmente enviadas ao cliente de email. Depois de ser transferida a última parte da mensagem, ela será verificada quanto a ameaças. Contudo, o risco de infecção aumenta com esse nível de controle. O nível de limpeza e o processamento de mensagens de marca (alertas de notificação anexos à linha de assunto e ao corpo dos emails) são idênticos à configuração de eficiência máxima.

Com o nível **Compatibilidade máxima**, o usuário é avisado por uma janela de alerta, caso haja o recebimento de uma mensagem infectada. Não é adicionada nenhuma informação sobre arquivos infectados à linha de assunto ou ao corpo do email de mensagens entregues e as ameaças não são removidas automaticamente. A exclusão de ameaças deve ser feita pelo usuário a partir do cliente de email.

4.1.2.2 Integração com clientes de email

A integração do ESET Smart Security com os clientes de email aumenta o nível de proteção ativa contra códigos maliciosos em mensagens de email. Se o seu cliente de email for aceito, essa integração poderá ser ativada no ESET Smart Security. Se a integração estiver ativada, a barra de ferramentas Antispam do ESET Smart Security será inserida diretamente no cliente de email, permitindo uma proteção mais eficiente de email. As configurações de integração estão disponíveis utilizando **Configuração > Entrar na configuração avançada... > Diversos > Integração com clientes de email**. Essa janela de diálogo permite ativar a integração com os clientes de email aceitos. Os clientes de email atualmente aceitos incluem o Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.

Selecione a opção ***Desativar verificação de alteração na caixa de entrada*** se estiver notando uma redução na velocidade do sistema ao trabalhar com o seu cliente de email. Essa situação pode ocorrer ao fazer download de email do Kerio Outlook Connector Store.

A proteção de email é iniciada pela ativação da caixa de seleção **Ativar proteção de email** em **Configuração avançada (F5)** > **Antivírus e antispyware** > **Proteção de email**.

4.1.2.2.1 Anexar mensagens de marca ao corpo de um email

Todo email controlado pelo ESET Smart Security pode ser marcado por anexar uma mensagem de marca ao assunto ou ao corpo do email. Esse recurso aumenta o nível de credibilidade do endereço e, se alguma ameaça for detectada, fornece informações valiosas sobre o nível de ameaça de um email/remetente específico.

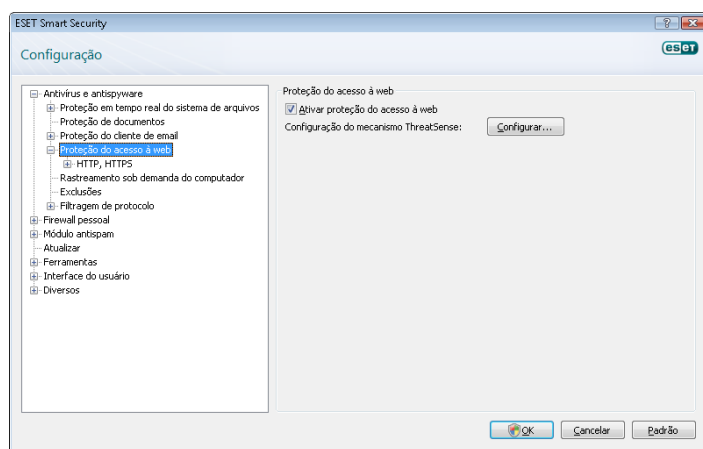
As opções dessa funcionalidade estão disponíveis através de **Configuração avançada > Antivírus e antispyware > Proteção de cliente de email**. O programa pode **Anexar mensagens de marca a emails recebidos e lidos**, bem como **Anexar mensagens de marca a emails enviados**. Os usuários podem também decidir se as mensagens de marca devem ser anexadas a todos os emails, somente aos emails infectados ou a nenhum email. O ESET Smart Security permite também ao usuário anexar mensagens ao assunto original das mensagens infectadas. Para permitir a anexação ao assunto, selecione as opções **Anexar observação ao assunto do email infectado recebido e lido** e **Anexar observação ao assunto do email infectado enviado**.

O conteúdo das notificações pode ser modificado no campo Modelo e acrescentado ao assunto do email infectado. As modificações mencionadas acima podem ajudar a automatizar o processo de filtragem de emails infectados, uma vez que elas permitem que você filtre emails com um assunto específico (se aceito pelo seu cliente de email) para uma pasta separada.

4.1.2.3 Remoção de ameaças

Se uma mensagem de email infectada for recebida, uma janela de alerta será exibida. A janela de alerta mostra o nome do remetente, o email e o nome da ameaça detectada. Na parte inferior da janela, as opções **Limpar**, **Excluir** ou **Deixar** estão disponíveis para o objeto detectado. Na maioria dos casos, recomendamos que você selecione **Limpar** ou **Excluir**. Em situações especiais, quando desejar receber o arquivo infectado, selecione **Deixar**. Se a **Limpeza rígida** estiver ativada, uma janela de informações sem nenhuma opção disponível para os objetos infectados será exibida.

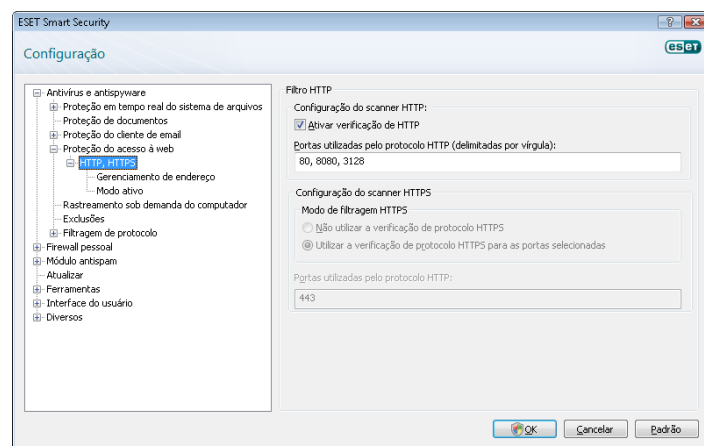
4.1.3 Proteção de acesso à web

A conectividade com a Internet é um recurso padrão em um computador pessoal. Infelizmente, ela tornou-se o principal meio para a transferência de códigos maliciosos. Por essa razão, é fundamental uma avaliação atenta de sua proteção de acesso à web. Recomendamos que a opção **Ativar proteção do acesso à web** esteja ativada. Essa opção está localizada em **Configuração avançada (F5) > Antivírus e antispyware > Proteção de acesso à web**.

4.1.3.1 HTTP, HTTPs

A proteção de acesso à web funciona monitorando a comunicação entre os navegadores da Internet e servidores remotos e cumprem as regras do protocolo HTTP (Hypertext Transfer Protocol) e HTTPs (comunicação criptografada). Por padrão, o ESET Smart Security está configurado para usar os padrões da maioria dos navegadores de Internet. Contudo, as opções de configuração do scanner HTTP podem ser modificadas em Proteção do acesso à web > HTTP, HTTPs. Na janela principal do filtro HTTP, é possível marcar ou desmarcar a opção **Ativar verificação de HTTP**. Você pode também definir os números das portas utilizadas para a comunicação HTTP. Por padrão, os números de portas 80, 8080 e 3128 estão predefinidos. A verificação de HTTPs pode ser executada nos seguintes modos:

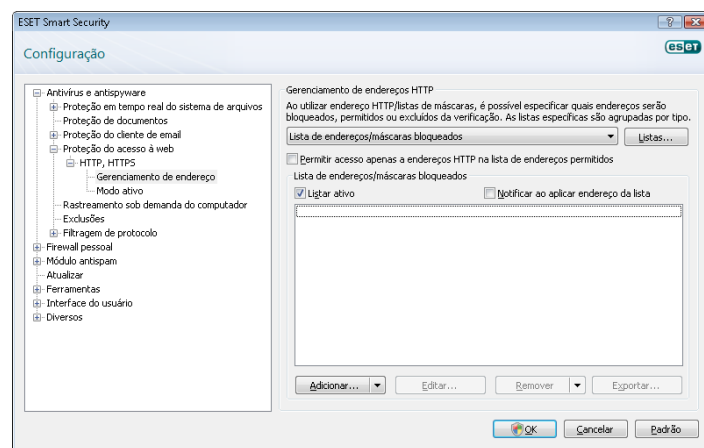
Não utilizar a verificação de protocolo HTTPs
A comunicação criptografada não será verificada

Utilizar a verificação de protocolo HTTPs para as portas selecionadas
Verificação de HTTPs apenas para as portas definidas em Portas utilizadas pelo protocolo HTTPs

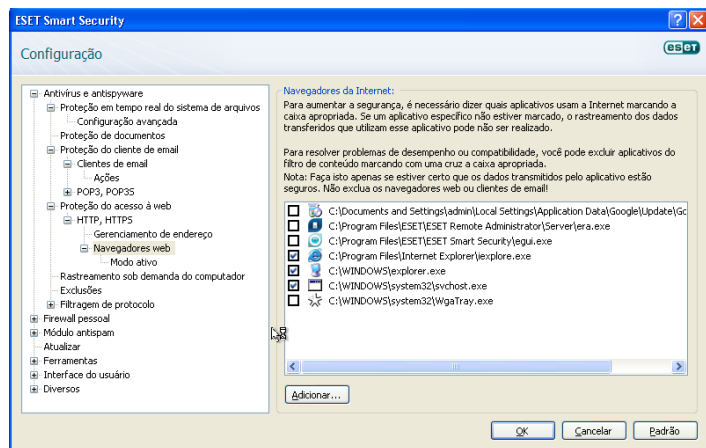
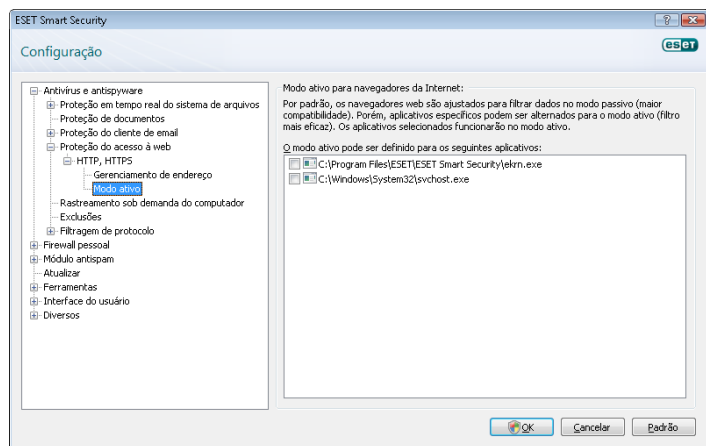
Utilizar a verificação de protocolo HTTPs para aplicativos marcados como navegadores da Internet que utilizam as portas selecionadas
Verificar apenas aqueles aplicativos que estão especificados na seção de navegadores e utilizar as portas definidas em ***Portas utilizadas pelo protocolo HTTPs***

4.1.3.1.1 Gerenciamento de endereços

Esta seção permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação

Os botões **Adicionar, Alterar, Remover** e **Exportar** são utilizados para gerenciar as listas de endereços. Os sites na lista de endereços bloqueados não serão acessíveis. Os sites na lista de endereços excluídos são acessados sem serem rastreados quanto a código malicioso. Se você ativar a opção ***Permitir acesso apenas a endereços HTTP na lista de endereços permitidos***, apenas endereços presentes na lista de endereços permitidos serão acessíveis, enquanto todos os outros endereços HTTP serão bloqueados.

Em todas as listas, os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco substitui qualquer sequência de caracteres e o ponto de interrogação substitui qualquer símbolo. Especial atenção deve ser prestada ao especificar os endereços excluídos, uma vez que a lista deve conter os endereços seguros e confiáveis. De modo semelhante, é necessário garantir que os símbolos * e ? sejam usados corretamente nesta lista. Para ativar uma lista, selecione a opção ***Lista ativa***. Se você desejar ser notificado ao entrar em um endereço da lista atual, selecione ***Notificar ao aplicar endereços da lista***.

4.1.3.1.2 Navegadores Web

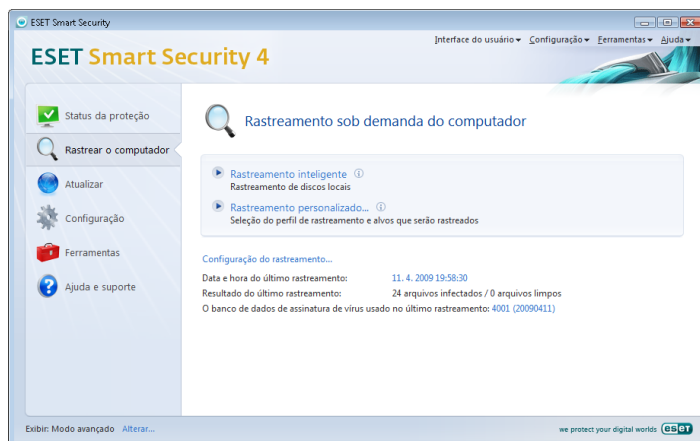
O ESET Smart Security contém também o recurso **Navegadores Web**, que permite que o usuário defina se determinado aplicativo é um navegador ou não. Se um aplicativo for marcado como um navegador pelo usuário, todas as comunicações desse aplicativo serão monitoradas, independentemente do número de portas envolvidas na comunicação.

Os recursos dos navegadores Web complementam o recurso de verificação HTTP, uma vez que a verificação HTTP acontece somente nas portas predefinidas. Entretanto, muitos serviços da Internet utilizam alterações dinâmicas ou números de porta desconhecidos. Para levar isso em conta, o recurso do navegador Web pode estabelecer o controle das comunicações das portas, independentemente dos parâmetros da conexão.

A lista de aplicativos marcados como navegadores pode ser acessada diretamente no submenu **Navegadores Web** da ramificação **HTTP**. Esta seção contém também o submenu **Modo ativo**, que define o modo de verificação para os navegadores da Internet. O **Modo ativo** é útil porque ele examina os dados transferidos como um todo. Se ele não estiver ativado, a comunicação dos aplicativos será monitorada gradualmente em lotes. Isso diminui a eficiência do processo de verificação dos dados, mas fornece também compatibilidade mais alta para os aplicativos listados. Se nenhum problema ocorrer ao usá-lo, recomendamos que você ative o modo de verificação ativo marcando a caixa de seleção ao lado do aplicativo desejado.

4.1.4 Rastreamento do computador

Caso suspeite que seu computador esteja infectado (se ele se comportar de maneira anormal), execute um rastreamento sob demanda para examinar se há ameaças no computador. Do ponto de vista da segurança, é fundamental que os rastreamentos do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. O rastreamento regular detecta ameaças que não foram detectadas pelo rastreador em tempo real quando foram salvas no disco. Isso pode acontecer caso a proteção em tempo real esteja desativada no momento da infecção ou se o banco de dados de assinatura de vírus estiver obsoleto.

Recomendamos que execute um Rastreamento sob demanda pelo menos uma ou duas vezes ao mês. O rastreamento pode ser configurado como uma tarefa em **Ferramentas > Agenda**.

4.1.4.1 Tipo de rastreamento

Há dois tipos disponíveis. O **Rastreamento padrão** verifica rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado...** permite ao usuário selecionar qualquer perfil de rastreamento predefinido, bem como escolher os objetos do rastreamento na estrutura em árvore.

4.1.4.1.1 Rastreamento padrão

O Rastreamento padrão é um método de fácil utilização que permite ao usuário iniciar rapidamente um rastreamento no computador e limpar arquivos infectados sem a necessidade de intervenção do usuário. Suas principais vantagens são a operação fácil, sem configurações de rastreamento detalhadas. O Rastreamento padrão verifica todos os arquivos em unidades locais e limpa ou exclui automaticamente ameaças detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte Limpeza (veja a página 20).

O perfil de rastreamento padrão foi elaborado para os usuários que desejam verificar de modo rápido e fácil seus computadores. Ele oferece um rastreamento eficiente e solução de limpeza sem exigir um extenso processo de configuração.

4.1.4.1.2 Rastreamento personalizado

O Rastreamento personalizado é uma solução excelente, caso queira especificar parâmetros de rastreamento adicionais, como alvos para rastreamento e métodos de rastreamento. A vantagem desse método é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que pode ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

Para selecionar alvos para rastreamento, use o menu suspenso do recurso de seleção rápida de alvos para rastreamento ou selecione os alvos na estrutura em árvore que lista todos os dispositivos disponíveis no computador. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração... > Limpeza**. Caso esteja interessado unicamente em rastrear o sistema sem realizar nenhuma outra ação, marque a caixa de seleção **Rastrear sem limpar**.

A realização de rastreamentos de computador com o modo Rastreamento personalizado é adequada para usuários avançados com experiência anterior no uso de programas antivírus.

4.1.4.2 Alvos para rastreamento

O menu suspenso Alvos para rastreamento permite selecionar arquivos, pastas e dispositivos (discos) para rastreamento quanto a vírus.

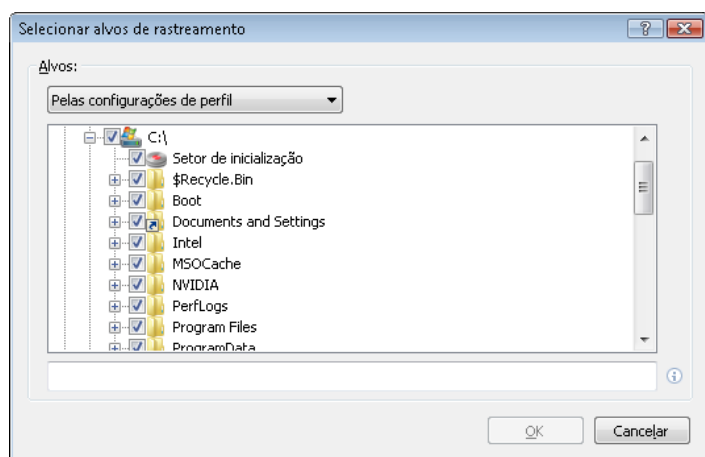
Com o uso da opção de menu rápido Alvos para rastreamento, é possível selecionar os seguintes alvos:

Configurações por perfil – controla alvos definidos no perfil de rastreamento selecionado

Mídia removível – disquetes, dispositivos de armazenamento USB, CD/DVD

Unidades locais – controla todas as unidades de disco rígido do sistema

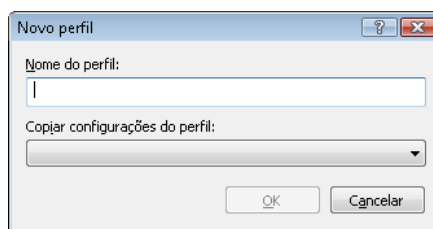
Unidades de rede – todas as unidades mapeadas

Nenhuma seleção – cancela todas as seleções

Um alvo para rastreamento pode ser também mais exatamente especificado através da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir no rastreamento. Selecione alvos na estrutura em árvore que lista todos os dispositivos disponíveis no computador.

4.1.4.3 Perfis de rastreamento

Os parâmetros de rastreamento de computador preferidos podem ser salvos nos perfis. A vantagem de criar perfis de rastreamento é que eles podem ser usados regularmente para rastreamento futuro. Recomendamos a criação de tantos perfis (com vários alvos para rastreamento, métodos de rastreamento e outros parâmetros) quantos o usuário utilize regularmente.

Para criar um novo perfil que possa ser usado repetidas vezes em rastreamentos futuros, navegue até **Configuração avançada** (F5) **> Rastreamento sob demanda do computador**. Clique no botão **Perfis...**, à direita, para exibir a lista de perfis de rastreamento existentes e a opção para criar um novo perfil. A seguinte **Configuração de parâmetros do mecanismo ThreatSense** descreve cada parâmetro da configuração de rastreamento. Isso o ajudará a criar um perfil de rastreamento que atenda às suas necessidades.

Exemplo:
Imagine que você queira criar seu próprio perfil de rastreamento e que a configuração atribuída ao perfil **Rastreamento inteligente** seja parcialmente adequada. Mas você não deseja rastrear empacotadores em tempo de execução ou aplicativos potencialmente inseguros e você também deseja aplicar **Limpeza rígida**. Na janela **Perfis de configuração**, clique no botão **Adicionar...** Digite o nome do seu novo perfil no campo **Nome do perfil** e selecione **Rastreamento inteligente** no menu suspenso **Copiar configurações do perfil:**. Em seguida, ajuste os demais parâmetros de modo a atender às suas necessidades.

4.1.5 Filtragem de protocolos

A proteção antivírus para os protocolos POP3 e HTTP do aplicativo é fornecida pelo mecanismo de rastreamento ThreatSense, que integra perfeitamente todas as técnicas avançadas de rastreamento de malware. O controle funciona automaticamente, independentemente dos navegadores da Internet ou cliente de email utilizado. As seguintes opções estão disponíveis para filtragem de protocolos (se a opção **Ativar filtragem de protocolos do aplicativo** estiver ativada:

Portas HTTP e POP3 - limita o rastreamento da comunicação com as portas HTTP e POP3 conhecidas.

Aplicativos marcados como navegadores da Internet e clientes de email – ative essa opção apenas para filtrar a comunicação de aplicativos marcados como navegadores (Proteção do acesso à web > HTTP, HTTPS > Navegadores web) e clientes de email (Proteção de cliente de email > POP3, POP3S > Clientes de email)

Portas e aplicativos marcados como navegadores da Internet ou clientes de email – verifica-se se há malware nas portas e nos navegadores

Observação:
Começando no Windows Vista Service Pack 1 e no Windows Server 2008, uma nova filtragem de comunicação é utilizada. Como resultado, a seção Filtragem de protocolos não está disponível.

4.1.5.1 SSL

O ESET Smart Security 4 permite verificar os protocolos encapsulados no protocolo SSL. É possível utilizar diversos modos de rastreamento para comunicações protegidas por SSL utilizando certificados confiáveis, certificados desconhecidos ou certificados que são excluídos da verificação da comunicação protegida por SSL.

Sempre rastrear o protocolo SSL (certificados excluídos e confiáveis permanecerão válidos) – selecione essa opção para rastrear todas as comunicações protegidas por SSL, exceto as comunicações protegidas por certificados excluídos da verificação. Se uma nova comunicação que utiliza um certificado desconhecido e assinado for estabelecida, o usuário não será notificado sobre o fato, e a comunicação será filtrada automaticamente. Quando o usuário acessar um servidor com um certificado não confiável que é marcado pelo usuário como confiável (ele é adicionado à lista de certificados confiáveis), a comunicação com o servidor é permitida e o conteúdo do canal de comunicação é filtrado.

Perguntar sobre sites não visitados (certificados desconhecidos) – se você entrar em um novo site protegido por SSL (com um certificado desconhecido), uma caixa de diálogo de seleção de ação será exibida. Esse modo possibilita criar uma lista de certificados SSL que serão excluídos do rastreamento.

Não rastrear o protocolo SSL – se a opção for selecionada, o programa não rastreará as comunicações em SSL

Caso o certificado não possa ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis:

Perguntar sobre validade de certificação – solicita que o usuário selecione uma ação a ser tomada

Bloquear a comunicação que utiliza o certificado – encerra a conexão com o site que utiliza o certificado

Se o certificado for inválido ou estiver corrompido

Perguntar sobre validade do certificado – solicita que o usuário selecione uma ação a ser tomada

Bloquear a comunicação que utiliza o certificado – encerra a conexão com o site que utiliza o certificado

4.1.5.1.1 Certificados confiáveis

Além do armazenamento de Autoridades de certificação raiz confiáveis, em que o ESET Smart Security 4 armazena certificado confiável, é possível criar uma lista personalizada de certificados confiáveis que podem ser visualizados em **Configuração** (F5) **> Filtragem de protocolos > SSL > Certificados confiáveis**.

4.1.5.1.2 Certificados excluídos

A seção Certificados excluídos contém certificados que são considerados seguros. O programa não verificará o conteúdo das comunicações criptografadas que utilizam certificados desta lista. Recomendamos a instalação apenas daqueles certificados da web que, com certeza, são seguros e que não precisem da execução da filtragem de conteúdo.

4.1.6 Configuração de parâmetros do mecanismo ThreatSense

ThreatSense é o nome da tecnologia que consiste em métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela fornece também proteção durante as primeiras horas da propagação de uma nova ameaça. Ela utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense elimina com êxito também os rootkits.

As opções de configuração da tecnologia ThreatSense permitem que o usuário especifique diversos parâmetros de rastreamento:

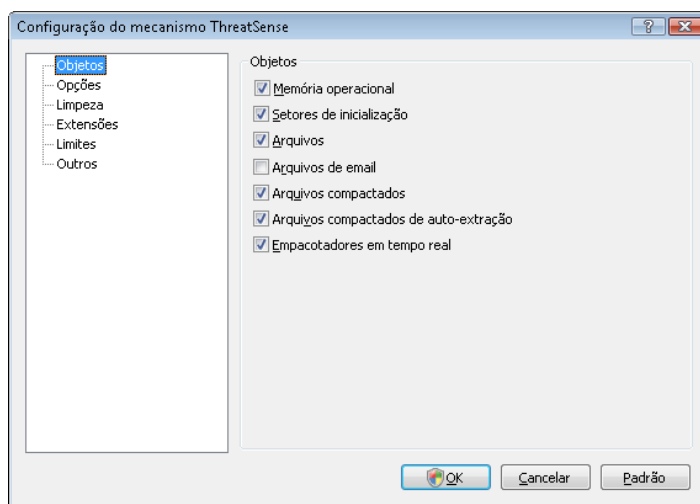
- Tipos e extensões de arquivos que serão rastreados
- A combinação de diversos métodos de detecção
- Níveis de limpeza, etc.

Para entrar na janela de configuração, clique no botão **Configuração...** localizado na janela de configuração de qualquer módulo que utiliza a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- Proteção em tempo real do sistema de arquivos
- Verificação de arquivo na inicialização do sistema
- Proteção de email
- Proteção de acesso à web
- Rastreamento sob demanda do computador

Os parâmetros do ThreatSense são altamente otimizados para cada módulo e a modificação deles pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre rastrear empacotadores em tempo de execução ou ativar heurística avançada no módulo de proteção do sistema de arquivos em tempo real pode resultar em redução da velocidade do sistema (normalmente, somente arquivos recém-criados são rastreados utilizando esses métodos). Portanto, recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto o módulo Rastrear o computador.

4.1.6.1 Configuração dos objetos

A seção **Objetos** permite definir quais componentes do computador e arquivos serão verificados quanto a ameaças.

Memória operacional – Rastreia quanto a ameaças que atacam a memória operacional do sistema.

Setores de inicialização – Rastreia os setores de inicialização quanto à presença de vírus no registro principal de inicialização

Arquivos – Fornece o rastreamento de todos os tipos de arquivos comuns (programas, imagens, áudio, arquivos de vídeo, arquivos de banco de dados, etc.)

Arquivos de email – Rastreia arquivos especiais que contêm mensagens de email

Arquivos compactados – Fornece o rastreamento de arquivos compactados em arquivos mortos (.rar, .zip, .arj, .tar, etc.)

Arquivos compactados de extração automática – Rastreia arquivos contidos em arquivos compactados de extração automática, mas que normalmente possuem a extensão .exe

Empacotadores em tempo de execução – os empacotadores em tempo de execução (diferentemente dos tipos de arquivos de compactação padrão) descompactam na memória, além dos empacotadores estáticos padrão (UPX, yoda, ASPack, FGS, etc.).

4.1.6.2 Opções

Na seção Opções, o usuário pode selecionar os métodos a serem usados ao rastrear o sistema em busca de ameaças. As seguintes opções estão disponíveis:

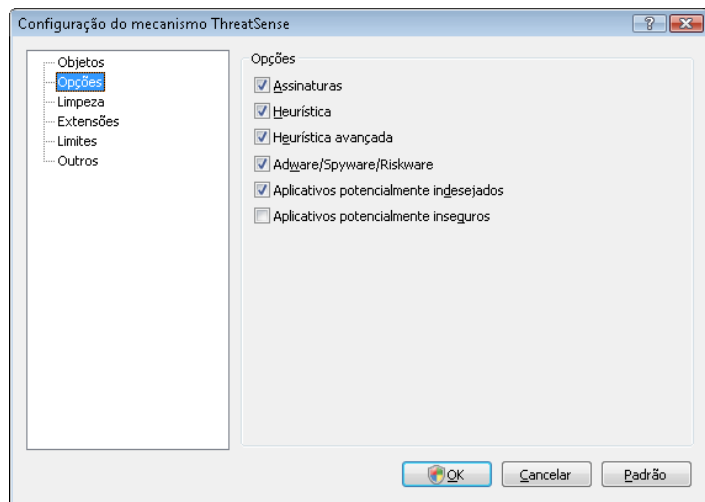
Assinaturas – As assinaturas podem detectar e identificar ameaças pelo nome, com exatidão e confiabilidade, usando as assinaturas de vírus.

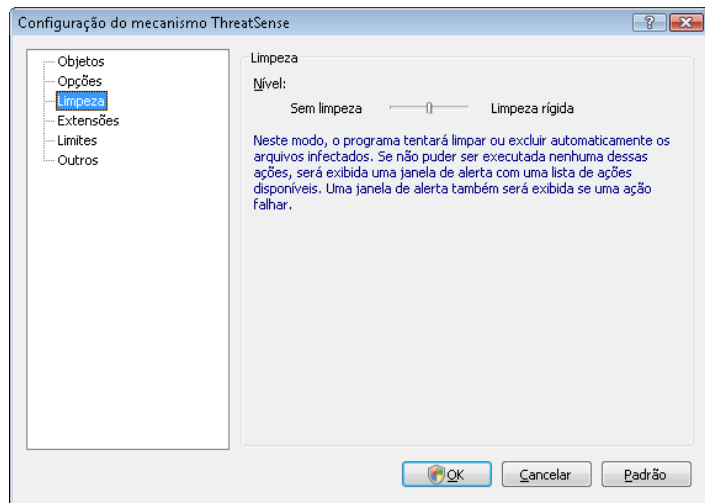
Heurística – A heurística é um algoritmo que analisa a atividade (maliciosa) de programas. A principal vantagem da detecção heurística é a capacidade de detectar novos softwares maliciosos, que não existiam antes ou não estavam incluídos na lista de vírus conhecidos (banco de dados de assinatura de vírus).

Heurística avançada – A heurística avançada é formada por um algoritmo heurístico exclusivo, desenvolvido pela ESET e otimizado para a detecção de vírus e cavalos de Troia de computador escritos em linguagens de programação de alto nível. Devido à heurística avançada, a inteligência de detecção do programa é significativamente maior.

Adware/Spyware/Riskware– Essa categoria inclui software que coleta várias informações sensíveis sobre usuários sem conhecimento ou consentimento dos mesmos. E inclui, ainda, software que exibe material de propaganda.

Aplicativos potencialmente inseguros – Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Inclui programas como ferramentas de acesso remoto, motivo pelo qual essa opção, por padrão, é desativada.

Aplicativos potencialmente indesejados – Aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de maneira negativa. Tais aplicativos geralmente exigem consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de forma diferente (em comparação ao estado antes da instalação). As alterações mais significativas são janelas pop-up indesejadas, ativação e execução de processos ocultos, aumento do uso de recursos do sistema, modificações nos resultados de pesquisa e aplicativos se comunicando com servidores remotos.

4.1.6.3 Limpeza

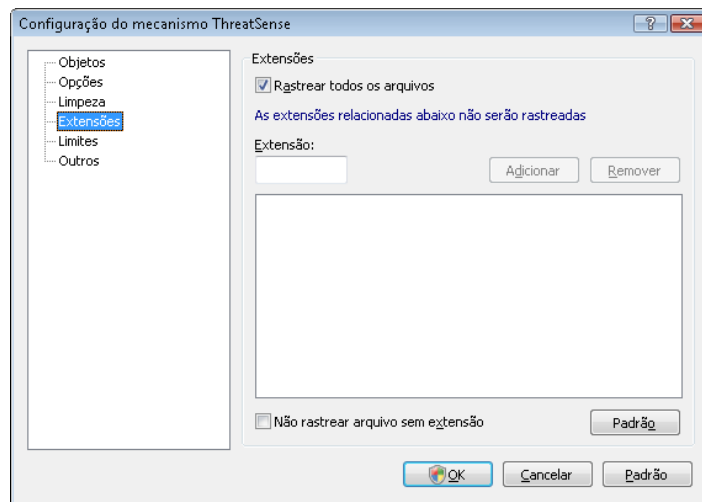
As configurações de limpeza determinam o comportamento do rastreador durante a limpeza de arquivos infectados. Há três níveis de limpeza:

Sem limpeza
Os arquivos infectados não são limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação.

Nível padrão
O programa tentará limpar ou excluir automaticamente um arquivo infectado. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá uma opção de ações a serem seguidas. A opção de ações a serem seguidas será exibida também se uma ação predefinida não puder ser concluída.

Limpeza rígida
O programa limpará ou excluirá todos os arquivos infectados (incluindo os arquivos mortos). As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, uma ação a ser tomada será sugerida ao usuário em uma janela de aviso.

Aviso:
No modo Padrão, o arquivo compactado inteiro será excluído somente se todos os arquivos do arquivo compactado estiverem infectados. Se o arquivo compactado contiver arquivos legítimos, ele não será excluído. Se um arquivo compactado infectado for detectado no modo Limpeza rígida, o arquivo compactado inteiro será excluído, mesmo se houver arquivos limpos.

4.1.6.4 Extensões

Extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Esta seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento. Se a opção **Rastrear todos os arquivos** não estiver marcada, a lista será alterada para mostrar todas as extensões de arquivo atualmente rastreadas. Com os botões **Adicionar** e **Remover**, você pode ativar ou desativar o rastreamento das extensões desejadas.

Para ativar o rastreamento de arquivos sem nenhuma extensão, selecione a opção **Rastrear arquivos sem extensão**.

A exclusão de arquivos do rastreamento pode ser útil se o rastreamento de determinados tipos de arquivos provocar a operação incorreta do programa que usa as extensões. Por exemplo, você poderá ser aconselhado a excluir as extensões EDB, EML e TMP se usar o servidor MS Exchange.

4.1.6.5 Limites

A seção Limites permite especificar o tamanho máximo de objetos e o nível de compactação de arquivos compactados a serem rastreados:

Tamanho máximo de objeto (bytes)
Define o tamanho máximo de objetos a serem rastreados. O módulo antivírus determinado rastreará apenas objetos menores do que o tamanho especificado. Não recomendamos alterar o valor padrão, pois não há razão para modificá-lo. Essa opção será alterada apenas por usuários avançados que podem ter razões específicas para excluir objetos maiores do rastreamento.

Tempo máximo do rastreamento para objeto (s)
Define o valor de tempo máximo para rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto após o tempo decorrido, independentemente da conclusão do rastreamento.

Nível de aninhamento de arquivos compactados
Especifica a profundidade máxima do rastreamento de arquivos compactados. Não recomendamos alterar o valor padrão de 10; sob circunstâncias normais, não haverá razão para modificá-lo. Se o rastreamento for encerrado prematuramente devido ao número de arquivos aninhados, o arquivo compactado permanecerá desmarcado.

Tamanho máximo de arquivo em arquivo compactado (bytes)
Essa opção permite especificar o tamanho máximo de arquivos contidos em arquivos compactados (quando forem extraídos) a serem rastreados. Se o rastreamento de um arquivo compactado for encerrado prematuramente por essa razão, o arquivo compactado permanecerá desmarcado.

4.1.6.6 Outro

Rastrear os fluxos de dados alternativos (ADS)
Os fluxos de dados alternativos (ADS) usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas ameaças tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

Executar rastreamento em segundo plano com baixa prioridade
Cada sequência de rastreamento consome uma determinada quantidade de recursos do sistema. Se você trabalhar com programas que demandam uma alta quantidade de recursos do sistema, poderá ativar o rastreamento em segundo plano com baixa prioridade e economizar recursos para os seus aplicativos.

Relatar todos os objetos
Se essa opção estiver selecionada, o relatório mostrará todos os arquivos rastreados, mesmo os não infectados.

Manter último registro de acesso
Marque essa opção para manter o tempo de acesso original dos arquivos rastreados, em vez de atualizá-lo (por exemplo, para uso com sistemas de backup de dados).

Relatório de rolagem
Essa opção permite que você ative/desative o rolamento do relatório. Se selecionada, as informações rolam para cima dentro da janela de exibição.

Exibir notificação sobre a conclusão do rastreamento em uma janela separada
Abra uma janela separada contendo informações sobre resultados do rastreamento.

4.1.7 Uma ameaça foi detectada

As ameaças podem alcançar o sistema a partir de vários pontos: páginas da web, arquivos compartilhados, email ou dispositivos removíveis (USB, discos externos, CDs, DVDs, disquetes, etc.).

Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, recomendamos que você faça o seguinte:

- Abra o ESET Smart Security e clique em **Rastrear o computador**
- Clique em **Rastreamento padrão** (para obter mais informações, consulte Rastreamento padrão).
- Quando o rastreamento tiver terminado, revise o relatório para obter informações como número de arquivos rastreados, infectados e limpos.

Se desejar rastrear apenas uma parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

Como exemplo geral de como as ameaças são manuseadas no ESET Smart Security, suponha que uma ameaça seja detectada pelo monitor do sistema de arquivo em tempo real, que usa o nível de limpeza Padrão. Ele tentará limpar ou excluir o arquivo. Se não houver uma ação predefinida a ser tomada para o módulo de proteção em tempo real, será solicitado a você que selecione uma opção na janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Deixar** estão disponíveis. A seleção da opção **Deixar** não é recomendada, visto que os arquivos infectados são mantidos intocados. A exceção a isso é quando você tem certeza de que o arquivo é inofensivo e foi detectado por engano.

Limpeza e exclusão
Aplique a limpeza se um arquivo limpo tiver sido atacado por um vírus que anexou um código malicioso a esse arquivo. Se esse for o caso, tente primeiro limpar o arquivo infectado, a fim de restaurá-lo ao seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Se um arquivo infectado estiver "bloqueado" ou em uso pelo processo do sistema, ele somente será excluído depois de ter sido liberado (geralmente após o reinício do sistema).

Exclusão de arquivos em arquivos compactados
No modo de limpeza Padrão, o arquivo compactado inteiro será excluído somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Entretanto, tome cuidado ao realizar um rastreamento de Limpeza rígida – com esse tipo de limpeza o arquivo será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

4.2 Firewall pessoal

O Firewall pessoal controla todo o tráfego de rede para e a partir do sistema. Isso é realizado por meio da permissão ou proibição de conexões individuais de rede, com base em regras de filtragem especificadas. Ele fornece proteção contra ataques de computadores remotos e ativa o bloqueio de alguns serviços. Fornece também proteção antivírus para protocolos HTTP e POP3. Essa funcionalidade representa um elemento muito importante de segurança do computador.

4.2.1 Modos de filtragem

Cinco modos de filtragem estão disponíveis no Firewall pessoal do ESET Smart Security. O comportamento do firewall é alterado com base no modo selecionado. Os modos de filtragem influenciam também o nível de interação necessário do usuário.

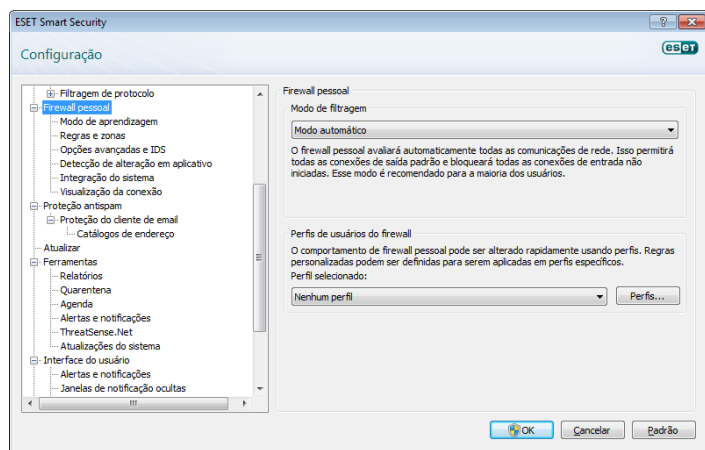
A filtragem pode ser executada de um dos cinco modos:

Modo automático – O modo padrão. Ele é adequado para usuários que preferem o uso fácil e conveniente do firewall sem nenhuma necessidade de definir regras. O Modo automático permite todo o tráfego de saída para determinado sistema e bloqueia todas as novas conexões iniciadas a partir do lado da rede.

Modo automático com exceções (regras definidas pelo usuário) – Além do modo Automático, ele permite adicionar regras personalizadas.

Modo interativo – Permite criar uma configuração feita sob medida para o seu Firewall pessoal. Quando uma conexão for detectada e não existir nenhuma regra que se aplique a essa comunicação, uma janela de diálogo que informa uma conexão desconhecida será exibida. A janela de diálogo oferece a opção de permitir ou proibir a comunicação, e a decisão de permitir ou proibir pode ser lembrada como uma nova regra para o Firewall pessoal. Se você optar por criar uma nova regra neste momento, todas as futuras conexões desse tipo serão permitidas ou bloqueadas, de acordo com a regra.

Modo com base em políticas – Bloqueia todas as conexões que não são definidas por uma regra específica que as permite. Esse modo permite que os usuários avançados definam as regras que permitem apenas as conexões desejadas e seguras. Todas as outras conexões não especificadas serão bloqueadas pelo Firewall pessoal.

Modo de aprendizagem – Cria e salva automaticamente as regras; esse modo é adequado para a configuração inicial do Firewall pessoal. Nenhuma interação com o usuário é exigida, porque o ESET Smart Security salva as regras de acordo com os parâmetros predefinidos. O Modo de aprendizagem não é seguro e deve ser usado apenas até que todas as regras para as comunicações exigidas tenham sido criadas.

4.2.2 Perfis

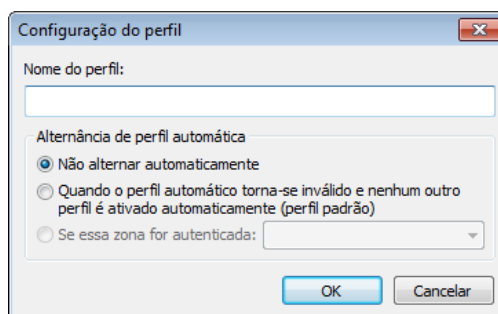
Perfis são uma ferramenta para controlar o comportamento do Firewall pessoal do ESET Smart Security. Ao criar ou editar uma regra de Firewall pessoal, você pode atribuí-la a um perfil específico ou aplicá-la a cada perfil. Quando você seleciona um perfil, apenas as regras globais (sem nenhum perfil especificado) e as regras que foram atribuídas a esse perfil são aplicadas. Você pode criar vários perfis com regras diferentes atribuídas para alterar com facilidade o comportamento do Firewall pessoal.

4.2.2.1 Gerenciamento de perfis

Clique no botão **Perfis...** (veja a figura na seção 4.2.1, "Modos de filtragem") para abrir a janela **Perfis do firewall**, em que você pode **Adicionar...**, **Editar** e **Remover** perfis. Observe que para **Editar** ou **Remover** um perfil, ele não pode estar selecionado no menu suspenso **Perfil selecionado**. Ao adicionar ou editar um perfil, você pode também definir as condições que o acionam. As seguintes possibilidades estão disponíveis:

Não alternar automaticamente – O acionador automático está desativado (o perfil deve ser ativado manualmente).

Quando o perfil automático torna-se inválido e nenhum outro perfil é ativado automaticamente (perfil padrão) – Quando o perfil automático torna-se inválido (se o computador estiver conectado a uma rede não confiável – consulte a seção 4.2.6.1, "Autenticação de rede") e nenhum outro perfil for ativado em seu lugar (o computador não estiver conectado a outra rede confiável), o Firewall pessoal alternará para esse perfil. Apenas um perfil pode usar esse acionador.

Se essa zona for autenticada – Esse perfil será acionado quando a zona especificada for autenticada (consulte a seção 4.2.6.1, "Autenticação de rede").

Quando o Firewall pessoal alternar para outro perfil, uma notificação será exibida no canto inferior direito próximo ao relógio do sistema.

4.2.3 Bloquear todo o tráfego de rede: desconectar a rede

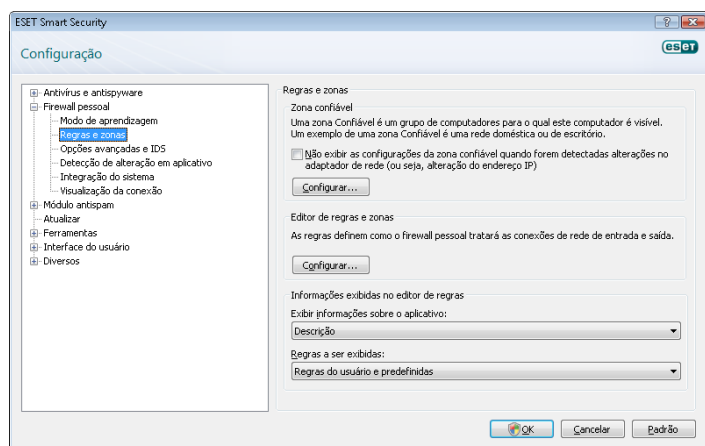
A única opção para bloquear todo o tráfego de rede é utilizar a opção **Bloquear todo o tráfego de rede: desconectar a rede**. Toda comunicação de entrada e de saída é bloqueada pelo Firewall pessoal sem nenhuma exibição de aviso. Utilize essa opção somente se suspeitar de riscos de segurança críticos que exijam a desconexão do sistema da rede.

4.2.4 Desativar filtragem: permitir todo o tráfego

A opção Desativar filtragem é a configuração oposta do bloqueio de todo o tráfego de rede. Se essa opção for selecionada, todas as opções de filtragem do Firewall pessoal serão desativadas, e todas as conexões de entrada e de saída serão permitidas. Ela terá o mesmo efeito, uma vez que nenhum firewall estará presente.

4.2.5 Configuração e uso de regras

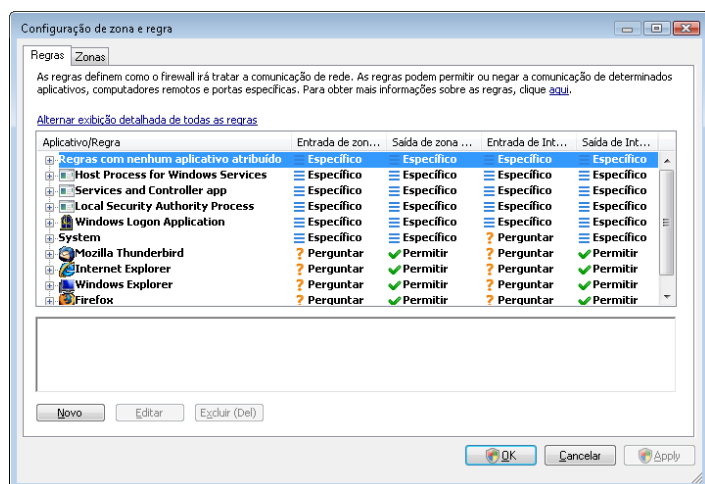
As regras representam um conjunto de condições utilizadas para testar significativamente todas as conexões de rede e todas as ações atribuídas a essas condições. Com o Firewall pessoal, é possível definir a ação a ser tomada, se uma conexão definida por uma regra for estabelecida.

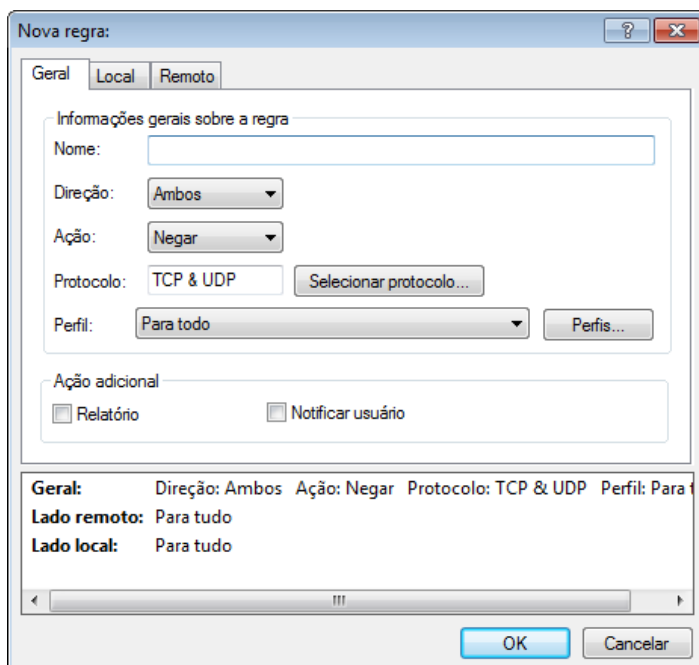
Para acessar a configuração de filtragem de regras, navegue até **Configuração avançada** (F5) **> Firewall pessoal > Regras e zonas**. Para exibir a configuração atual, clique em **Configuração...** na seção **Editor de regras e zonas** (se o Firewall pessoal estiver configurado como **Modo automático**, essas configurações não estarão disponíveis).

Na janela **Configuração de zona e regra**, uma visão geral das regras ou zonas é exibida (com base na guia selecionada no momento). A janela é dividida em duas seções. A seção superior lista todas as regras em uma exibição reduzida. A seção inferior exibe detalhes sobre a regra selecionada no momento, na seção superior. Na parte mais inferior estão os botões **Novo**, **Editar** e **Excluir (Del)**, que permitem que o usuário configure as regras.

As conexões podem ser divididas em conexões de entrada e de saída. As conexões de entrada são iniciadas por um computador remoto que tenta estabelecer conexão com o sistema local. As conexões de saída funcionam de maneira oposta – o sistema local contata um computador remoto.

Se uma nova comunicação desconhecida for detectada, é preciso considerar cuidadosamente se vai permiti-la ou proibi-la. As conexões não solicitadas, não seguras ou desconhecidas representam um risco de segurança para o sistema. Se tal conexão for estabelecida, recomendamos que seja dada atenção especial ao lado remoto e à tentativa de o aplicativo se conectar ao computador. Muitas ameaças tentam obter e enviar dados particulares ou fazem download de outros aplicativos maliciosos para estações de trabalho host. O Firewall pessoal permite detectar e finalizar tais conexões.

4.2.5.1 Criação de uma nova regra

Ao instalar um novo aplicativo que acessa a rede ou ao modificar uma conexão existente (lado remoto, número da porta etc.), uma nova regra deve ser criada.

Para adicionar uma nova regra, verifique se a guia **Regras** está selecionada. Em seguida, clique no botão **Novo**, na janela **Configuração de zona e regra**. Ao clicar nesse botão, é aberta uma nova janela de diálogo para a especificação de uma nova regra. A parte superior da janela contém três guias:

- **Geral:** Especifique um nome de regra, a direção da conexão, a ação, o protocolo e o perfil ao qual a regra se aplicará.
- **Remoto:** Essa guia contém informações sobre a porta remota (intervalo de portas). Permite também definir uma lista de endereços IP remotos ou zonas de uma determinada regra.
- **Local:** Exibe informações sobre o lado local da conexão, incluindo o número da porta local ou o intervalo de portas e o nome do aplicativo de comunicação.

Um bom exemplo de adição de uma nova regra é permitir que o seu navegador da Internet acesse a rede. Os itens a seguir devem ser fornecidos neste caso:

- Na guia **Geral**, ative a comunicação de saída por meio do protocolo TCP e UDP
- Adicione o processo que representa o aplicativo do seu navegador (no Internet Explorer, é iexplore.exe) na guia **Local**
- Na guia **Remoto**, ative o número da porta 80 apenas se desejar permitir as atividades de navegação padrão na Internet.

4.2.5.2 Edição de regras

Para modificar uma regra existente, clique no botão Editar. Todos os parâmetros (consulte a seção 4.2.5.1 "Criação de novas regras") podem ser modificados.

A modificação é necessária toda vez que algum dos parâmetros monitorados for alterado. Nesse caso, a regra não pode atender às condições e a ação especificada não pode ser aplicada. No fim, a conexão pode ser recusada, o que pode resultar em problemas com a operação do aplicativo em questão. Um exemplo é uma alteração do endereço de rede ou do número de porta do lado remoto.

4.2.6 Configuração de zonas

Na janela **Configuração de zona**, você pode especificar o nome da zona, a descrição, a lista de endereços de rede e a autenticação de zona (consulte a seção 4.2.6.1.1, "Autenticação de zona – Configuração de cliente").

Uma zona representa uma coleção de endereços de rede que criam um grupo lógico. A cada endereço de um determinado grupo são atribuídas regras semelhantes definidas centralmente para todo o grupo. Um exemplo de tal grupo é a Zona confiável. A Zona confiável representa um grupo de endereços de rede que são de total confiança e não são bloqueados pelo Firewall pessoal de maneira alguma.

Essas zonas podem ser configuradas utilizando a guia **Zonas** na janela **Configuração de zona e regra**, clicando no botão **Novo**. Insira um Nome para a zona e uma **Descrição** e adicione um endereço IP remoto clicando no botão **Adicionar endereço IPv4**.

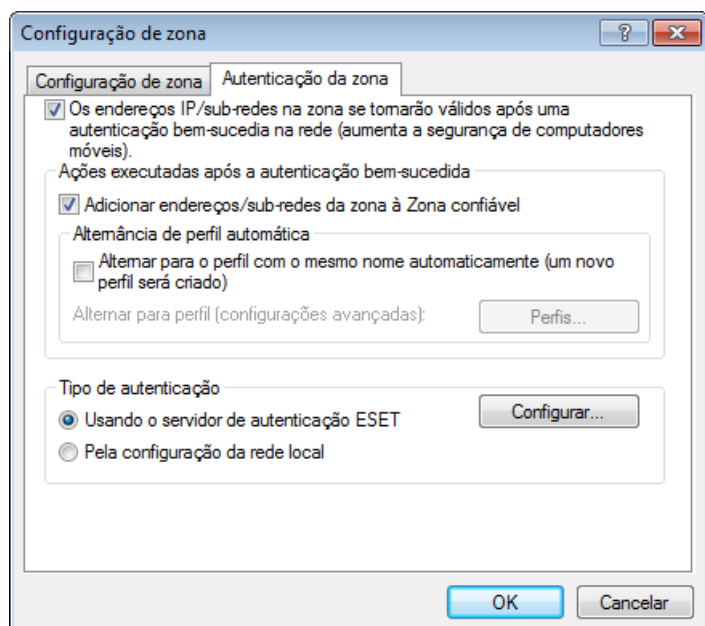
4.2.6.1 Autenticação de rede

A Zona confiável é identificada pelo endereço IP local do adaptador de rede. Os computadores móveis geralmente inserem redes com endereços IP semelhantes à rede confiável. Se as configurações da Zona confiável não forem alternadas manualmente para **Proteção rígida**, o Firewall pessoal continuará a usar o modo **Permitir compartilhamento**.

Para evitar esse tipo de situação, a Autenticação de zona procura por um servidor específico na rede e usa criptografia assimétrica (RSA) para autenticar o servidor. O processo de autenticação é repetido para cada rede à qual o computador se conecta.

4.2.6.1.1 Autenticação de zona – Configuração de cliente

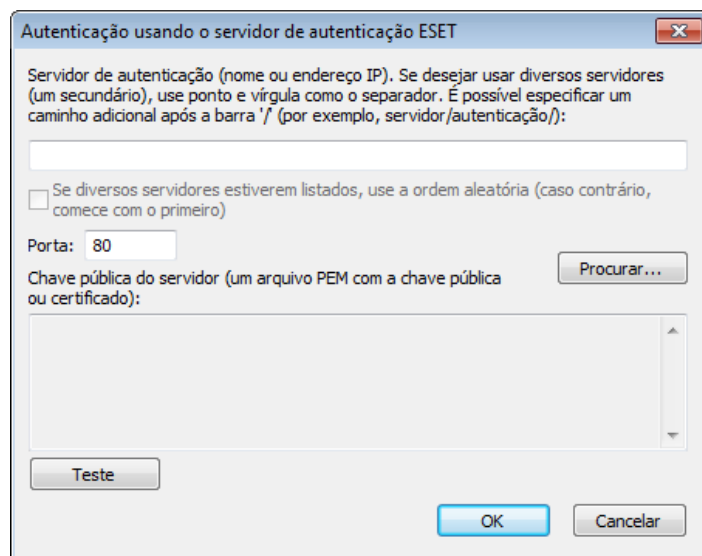
Na janela **Configuração de zona e regra**, clique na guia **Zona** e crie uma nova zona usando o nome da zona autenticada pelo servidor. Em seguida, clique em **Adicionar endereço IPv4** e selecione a opção **Sub-rede** para adicionar uma máscara de sub-rede que contenha o servidor de autenticação.

Clique na guia **Autenticação de zona** e selecione a opção **Os endereços IP/sub-redes na zona se tornarão válidos após uma autenticação bem-sucedida do servidor na rede**. Com essa opção selecionada, a zona se tornará inválida se a autenticação for malsucedida. Para selecionar um perfil de Firewall pessoal a ser ativado após uma autenticação bem-sucedida da zona, clique no botão **Perfis...** Se você selecionar a opção **Adicionar endereços/sub-redes da zona à Zona confiável**, os endereços/sub-redes da zona serão adicionados à Zona confiável após uma autenticação bem-sucedida (recomendado).

Há três tipos de autenticação disponíveis:

1) Usando o servidor de autenticação ESET

Clique em **Configuração...** e especifique um nome de servidor, uma porta de escuta do servidor e uma chave pública que corresponda à chave privada do servidor (consulte a seção 4.2.6.1.2, "Autenticação de zona – Configuração de servidor"). O nome do servidor pode ser inserido na forma de um endereço IP, um DNS ou um nome NetBios. O nome do servidor pode ser seguido por um caminho especificando o local da chave no servidor (por exemplo, nome_do_servidor_/diretório1/diretório2/autenticação). Insira vários servidores, separados por pontos e vírgulas, para atuar como servidores alternativos se o primeiro não estiver disponível.

A chave pública pode ser um arquivo de um dos seguintes tipos:

- Chave pública PEM codificada (.pem) - Essa chave pode ser gerada usando o Servidor de autenticação ESET (consulte a seção 4.2.6.1.2, "Autenticação de zona – Configuração de servidor").
- Chave pública codificada
- Certificado de chave pública (.crt)

Para testar suas configurações, pressione o botão **Testar**. Se a autenticação for bem-sucedida, será exibida uma mensagem *Autenticação do servidor bem-sucedida*. Se a autenticação não estiver configurada corretamente, será exibida uma das seguintes mensagens de erro:

Falha na autenticação do servidor. Tempo máximo para autenticação decorrido.
O servidor de autenticação está inacessível. Verifique o nome do servidor/endereço IP e/ou verifique as configurações do Firewall pessoal das seções do cliente e do servidor.

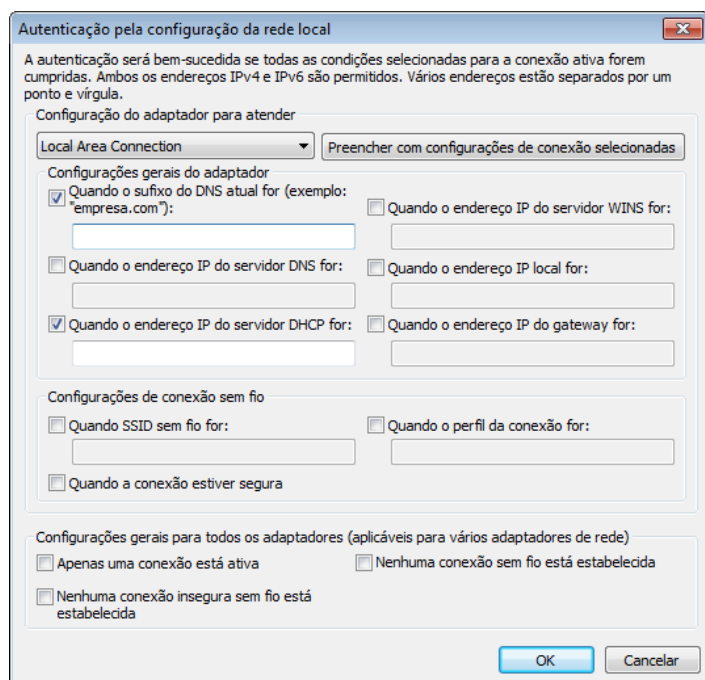
Ocorreu um erro ao comunicar com o servidor.
O servidor de autenticação não está em execução. Inicie o serviço do servidor de autenticação (consulte a seção 4.2.6.1.2, "Autenticação de zona – Configuração de servidor").

O nome da zona de autenticação não corresponde à zona do servidor.
O nome da zona configurada não corresponde à zona do servidor de autenticação. Revise as duas zonas e certifique-se de que seus nomes sejam idênticos.

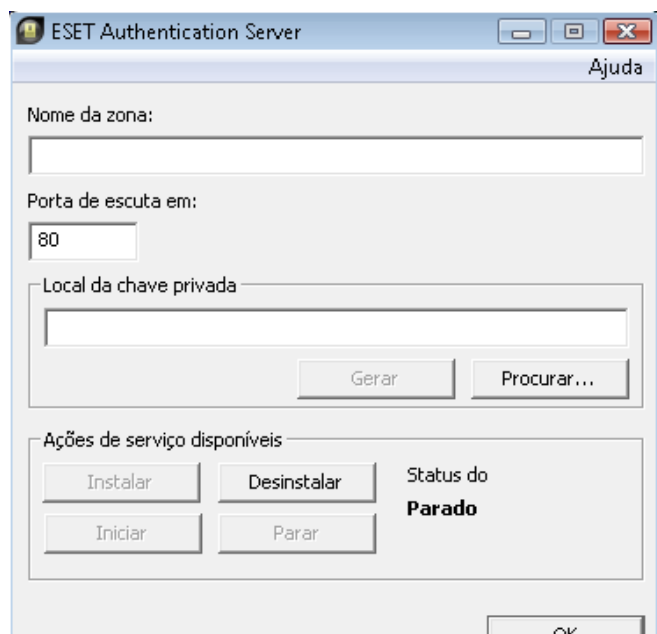
Falha na autenticação do servidor. O endereço do servidor não foi encontrado na lista de endereços da zona determinada.
O endereço IP do computador executando o servidor de autenticação está fora do intervalo de endereços IP definido da configuração atual da zona.

Falha na autenticação do servidor. Provavelmente uma chave pública inválida foi inserida.
Verifique se a chave pública especificada corresponde à chave privada do servidor. Verifique também se o arquivo de chave pública não está corrompido.

2) Pela configuração da rede local

A autenticação é executada de acordo com os parâmetros do adaptador de uma rede local. A autenticação será bem-sucedida se todos os parâmetros selecionados da conexão ativa forem válidos.

4.2.6.1.2 Autenticação de zona – Configuração de servidor

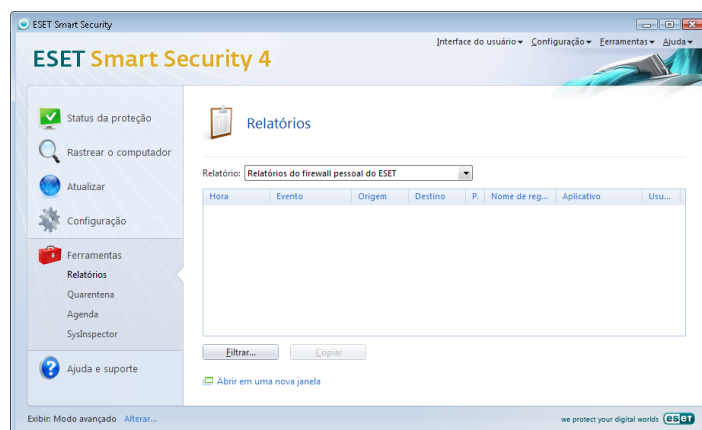
O processo de autenticação pode ser executado por qualquer computador/servidor conectado à rede que deva ser autenticado. O aplicativo Servidor de autenticação ESET precisa estar instalado em um computador/servidor que esteja sempre acessível para autenticação quando um cliente tentar se conectar à rede. O arquivo de instalação do aplicativo Servidor de autenticação ESET está disponível para download no site da ESET.

Depois de instalar o aplicativo Servidor de autenticação ESET, uma janela de diálogo será exibida (você pode acessar o aplicativo a qualquer momento em **Iniciar > Programas > ESET > Servidor de autenticação ESET > ESET Authentication Server**).

Para configurar o servidor de autenticação, insira o nome da zona de autenticação, a porta de escuta do servidor (o padrão é 80), bem como o local para armazenar o par de chaves pública e privada. Gere a chave pública e a chave privada que serão utilizadas no processo de autenticação. A chave privada permanecerá definida no servidor, enquanto a chave pública precisará ser importada no lado do cliente, na seção Autenticação de zona ao configurar uma zona na configuração do firewall.

4.2.7 Estabelecimento de uma conexão – detecção

O Firewall pessoal detecta cada conexão de rede recém-criada. O modo de firewall ativo determina quais ações serão executadas para a nova regra. Se Modo automático ou Modo com base em políticas estiver ativado, o Firewall pessoal executará ações predefinidas sem nenhuma interação com o usuário. O Modo interativo exibe uma janela de informações que relata a detecção de uma nova conexão de rede, suplementada com informações detalhadas sobre a conexão. Você pode optar por permitir a conexão ou recusá-la (bloqueá-la). Se permitir a mesma conexão várias vezes na janela de diálogo, recomendamos que crie uma nova regra para a conexão. Para fazer isso, selecione a opção **Lembrar ação** (Criar regra) e salve a ação como uma nova regra para o Firewall pessoal. Se o firewall reconhecer a mesma conexão no futuro, ele aplicará a regra existente.

Tenha cuidado ao criar novas regras e somente permita conexões que sejam seguras. Se todas as conexões forem permitidas, então o Firewall falhará em realizar seu propósito. Estes são os parâmetros importantes para as conexões:

- **Lado remoto:** Somente permita conexões para endereços confiáveis e conhecidos
- **Aplicativo local:** Não é aconselhável permitir conexões para aplicativos e processos desconhecidos
- **Número da porta:** A comunicação em portas comuns (por exemplo, tráfego da web – número da porta 80) deve ser permitida sob circunstâncias normais

A fim de se proliferarem, as ameaças de computador usam geralmente a Internet e conexões ocultas para ajudar a infectar sistemas remotos. Se as regras forem configuradas corretamente, um Firewall pessoal se tornará uma ferramenta útil para a proteção contra uma variedade de ataques de códigos maliciosos.

4.2.8 Relatórios

O Firewall pessoal do ESET Smart Security salva todos os eventos importantes em um relatório, que pode ser exibido diretamente a partir do menu principal. Clique em **Ferramentas > Relatórios** e selecione **Relatórios do Firewall pessoal da ESET** no menu suspenso **Relatório**.

Os relatórios são uma ferramenta valiosa para detectar erros e revelar intrusos dentro do sistema e devem receber atenção adequada. Os relatórios do Firewall pessoal da ESET contêm os seguintes dados:

- Data e hora do evento
- Nome do evento
- Origem
- Endereços de rede de destino
- Protocolo de comunicação de rede
- Regra aplicada ou nome do worm, se identificado
- Aplicativo envolvido
- Usuário

Uma análise completa desses dados pode ajudar a detectar tentativas de comprometer a segurança do sistema. Muitos outros fatores indicam riscos de segurança potenciais e permitem minimizar seus impactos: conexões muito frequentes de locais desconhecidos, diversas tentativas para estabelecer conexões, aplicativos desconhecidos comunicando-se e números de portas incomuns sendo utilizados.

4.3 Proteção antispam

Nos dias de hoje, os emails não solicitados (spams) estão entre os maiores problemas da comunicação eletrônica. Eles representam até 80% de toda a comunicação por email. A proteção Antispam serve para proteger contra esse problema. Combinando diversos princípios eficientes, o módulo Antispam fornece filtragem superior.

Um princípio importante na detecção do spam é a capacidade de reconhecer emails não solicitados com base em endereços confiáveis predefinidos (lista de permissões) e nos endereços de spam (lista de proibições). Todos os endereços do seu cliente de email são automaticamente acrescentados à Lista de permissões, bem como todos os demais endereços marcados pelo usuário como seguros.

O principal método usado para detectar spam é o rastreamento de propriedades da mensagem de email. As mensagens recebidas são verificadas quanto aos critérios Antispam básicos (definições da mensagem, heurística de estatísticas, reconhecimento de algoritmos e outros métodos únicos) e o valor do índice resultante determina se uma mensagem é ou não spam.

O filtro Bayesian também é utilizado na filtragem. Ao marcar as mensagens como *spam* e *não spam*, o usuário cria um banco de dados de palavras usadas em suas respectivas categorias. Quanto maior o banco de dados, maior a precisão dos resultados que ele produz.

A combinação dos métodos acima mencionados fornece um percentual de detecção antispam mais alto.

O ESET Smart Security suporta a proteção antispam para o Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.

4.3.1 Aprendizagem automática do Antispam

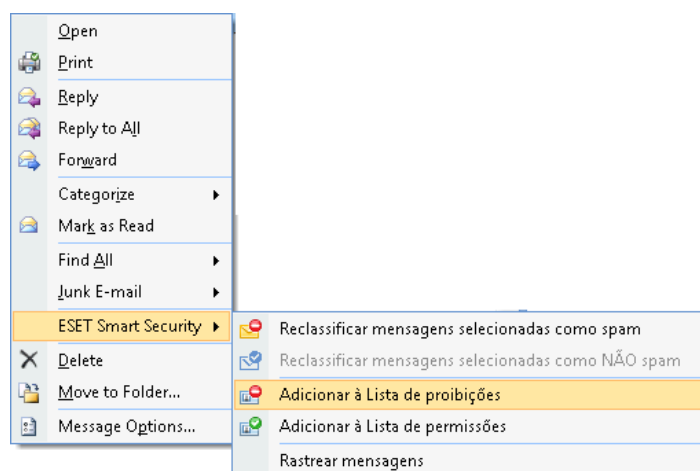
A aprendizagem automática do Antispam está relacionada ao filtro Bayesian mencionado anteriormente. A importância das palavras individuais muda durante o processo de "aprendizagem" de marcação das mensagens individuais como spam ou não spam. Da mesma forma, quanto mais mensagens classificadas (marcadas como spam ou não spam), mais precisos serão os resultados obtidos com o filtro Bayesian.

Acrescente endereços conhecidos à Lista de permissões para excluir mensagens desses endereços da filtragem.

4.3.1.1 Adição de endereços à Lista de permissões

Os endereços de email pertencentes às pessoas com as quais os usuários se comunicam com mais frequência podem ser acrescentados à lista de endereços "seguros" (Lista de permissões). Fazer isso assegura que nenhuma mensagem originária dos endereços da lista de permissões seja classificada como spam. Para adicionar um novo endereço à Lista de permissões, clique com o botão direito do mouse na mensagem de email e selecione **Adicionar à Lista de permissões** sob a opção do menu de contexto do ESET Smart Security ou clique em **Endereços confiáveis** na barra de ferramentas Antispam do ESET Smart Security na seção superior do seu programa de email. De modo semelhante, esse processo se aplica aos endereços de spam. Se um endereço de email for listado na lista de proibições, toda mensagem de email enviada daquele endereço será classificada como spam.

4.3.1.2 Marcação de mensagens como spam

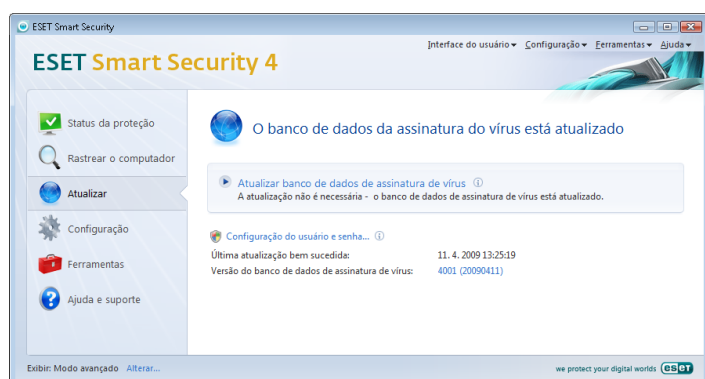
Qualquer mensagem exibida em seu cliente de email pode ser marcada como spam. Para fazer isso, use o menu de contexto (clique com o botão direito do mouse em **ESET Smart Security > Reclassificar mensagens selecionadas como spam**) ou clique em **Spam** na barra de ferramentas Antispam do ESET Smart Security, localizada em seu cliente de email.

As mensagens reclassificadas são automaticamente movidas para a pasta SPAM, mas o endereço do email do remetente não é acrescentado à lista de proibições. De modo semelhante, as mensagens podem ser classificadas como "não spam". Se as mensagens da pasta **Junk Email** forem classificadas como não spam, elas serão movidas para a sua pasta original. Marcar uma mensagem como não spam não acrescenta automaticamente o endereço do remetente à Lista de permissões.

4.4 Atualização do programa

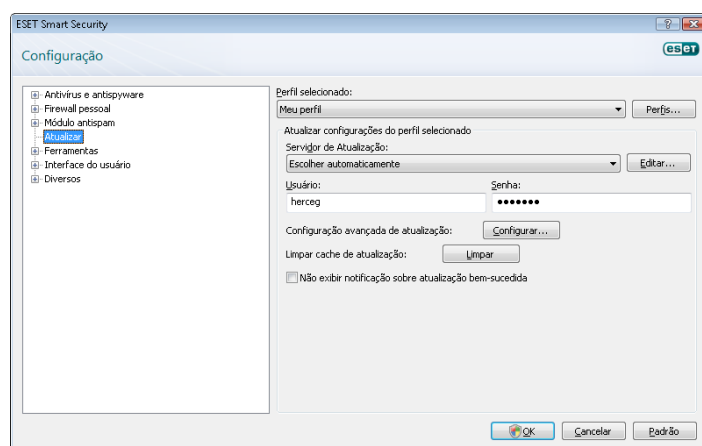
A atualização regular do sistema é o princípio básico para obter o nível máximo de segurança fornecido pelo ESET Smart Security. O módulo Atualização garante que o programa estará sempre atualizado. Isso é feito de duas maneiras – atualizando o banco de dados de assinatura de vírus e atualizando todos os componentes do sistema.

As informações sobre o status atual da atualização podem ser encontradas clicando em **Atualizar**, incluindo a versão atual do banco de dados de assinatura de vírus e se uma atualização será necessária. Além disso, a opção de ativar o processo imediato da atualização – **Atualizar banco de dados de assinatura de vírus** – está disponível, bem como as opções básicas de configuração da atualização, como, por exemplo, o nome do usuário e a senha para acessar os servidores de atualização da ESET.

A janela de informações contém também detalhes, como a data e hora da última atualização bem-sucedida e o número do banco de dados de assinatura de vírus. Essa indicação numérica é um link ativo para o site da ESET na web que lista todas as assinaturas adicionadas dentro da atualização específica.

Utilize o link **Registrar** para abrir o formulário de registro que possibilitará o registro de sua nova licença na ESET e, posteriormente, os dados de autenticação serão enviados para o seu email.

OBSERVAÇÃO: O Usuário e a Senha são fornecidos pela ESET após a compra do ESET Smart Security.

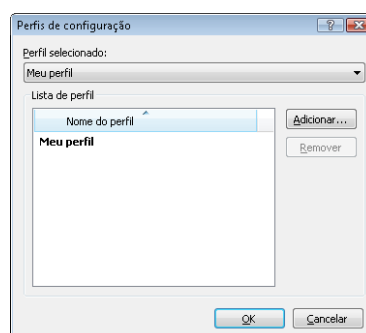
4.4.1 Configuração da atualização

Na seção de configuração da atualização você especifica as configurações da atualização, por exemplo, os servidores de atualização e os dados de autenticação desses servidores. Por padrão, o campo **Atualizar servidor:** está configurado como **Escolher automaticamente**. Esse valor assegura que será feito o download dos arquivos de atualização automaticamente a partir do servidor da ESET com a menor carga de tráfego de rede. As opções de configuração da atualização estão disponíveis em Configuração avançada (F5), em **Atualizar**.

A lista de servidores de atualização existentes no momento pode ser acessada utilizando o menu suspenso **Atualizar servidor:**. Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações para o perfil selecionado** e, em seguida, clique no botão **Adicionar**.

A autenticação nos servidores de atualização é concedida pelo **Nome de usuário** e pela **Senha** que foram gerados e enviados pela ESET para o usuário após a compra da licença do produto.

4.4.1.1 Atualizar perfis

Para várias configurações de atualização, é possível criar perfis de atualização, definidos pelo usuário, que podem ser utilizados para uma tarefa de atualização específica. A criação de vários perfis de atualização é especialmente útil para usuários móveis, uma vez que as propriedades de conexão à Internet mudam regularmente. Ao modificarem a tarefa de atualização, os usuários móveis podem especificar que, se não for possível atualizar o programa utilizando a configuração especificada em **Meu perfil**, a atualização será executada utilizando um perfil alternativo.

O menu suspenso **Perfil selecionado** exibe o perfil selecionado no momento. Por padrão, essa entrada é configurada como **Meu perfil**. Para criar um novo perfil, clique no botão **Perfis...** e, em seguida, clique no botão **Adicionar...** e digite seu próprio **Nome de perfil**. Ao criar um novo perfil, é possível copiar as configurações de um perfil existente selecionando-o no menu suspenso **Copiar configurações do perfil:**.

Dentro da configuração do perfil, é possível especificar o servidor de atualização ao qual o programa se conectará e fazer download de atualizações; qualquer servidor da lista de servidores disponíveis pode ser utilizado ou um novo servidor pode ser adicionado. A lista de servidores de atualização existentes pode ser acessada utilizando o menu suspenso **Atualizar servidor:**. Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações de perfil selecionado** e, em seguida, clique no botão **Adicionar**.

4.4.1.2 Configuração avançada de atualização

Para exibir a opção **Configuração avançada de atualização**, clique no botão **Configuração...** As opções de configuração avançada de atualização incluem a configuração de **Modo de atualização, Proxy HTTP, Rede local** e **Imagem**.

4.4.1.2.1 Modo de atualização

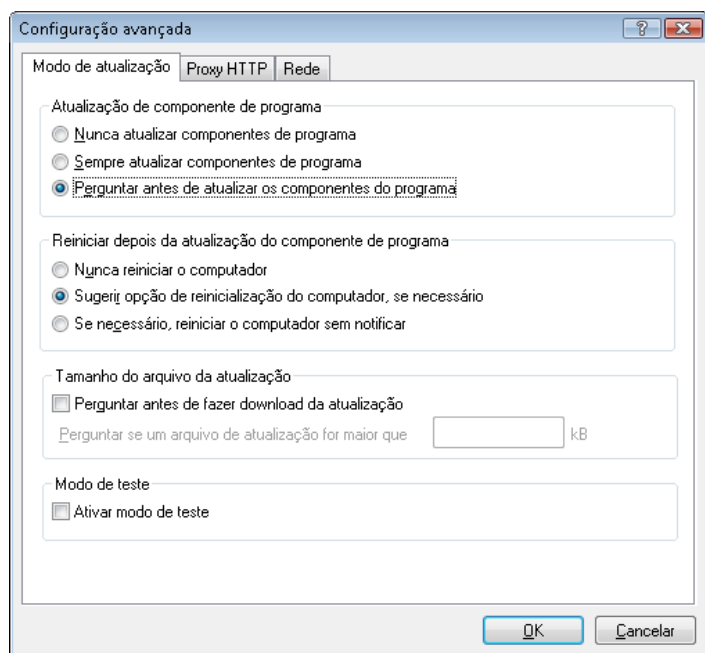
A guia **Modo de atualização** contém opções relacionadas à atualização de componentes do programa.

Na seção **Atualização de componente do programa**, há três opções disponíveis:

- **Nunca atualizar componentes do programa**
- **Sempre atualizar componentes do programa**
- **Perguntar antes de fazer download dos componentes do programa**

A escolha da opção **Nunca atualizar componentes do programa** garante que não será feito o download de uma nova atualização de componentes do programa liberados pela ESET, e nenhuma atualização de componentes do programa ocorrerá realmente na estação de trabalho. A opção **Sempre atualizar componentes do programa** significa que as atualizações de componentes do programa serão executadas sempre que uma nova atualização estiver disponível nos servidores de atualização da ESET e que os componentes do programa serão atualizados para a versão cujo download foi feito.

Selecione a terceira opção **Perguntar antes de fazer download dos componentes do programa** para garantir que o programa solicitará ao usuário a confirmação para iniciar o download das atualizações de componentes do programa no momento em que essas atualizações estiverem disponíveis. Nesse caso, uma janela de diálogo que contém informações sobre as atualizações de componentes do programa será exibida com a opção de confirmação ou de recusa. Se confirmada, será feito o download das atualizações e os novos componentes do programa serão instalados.

A opção padrão para a atualização de componentes do programa é **Perguntar antes de fazer download dos componentes do programa**.

Após a instalação de uma atualização de componentes do programa, é necessário reiniciar o sistema para obter total funcionalidade de todos os módulos. A seção **Reinicar após a atualização de componentes do programa** permite que o usuário selecione uma das três opções a seguir:

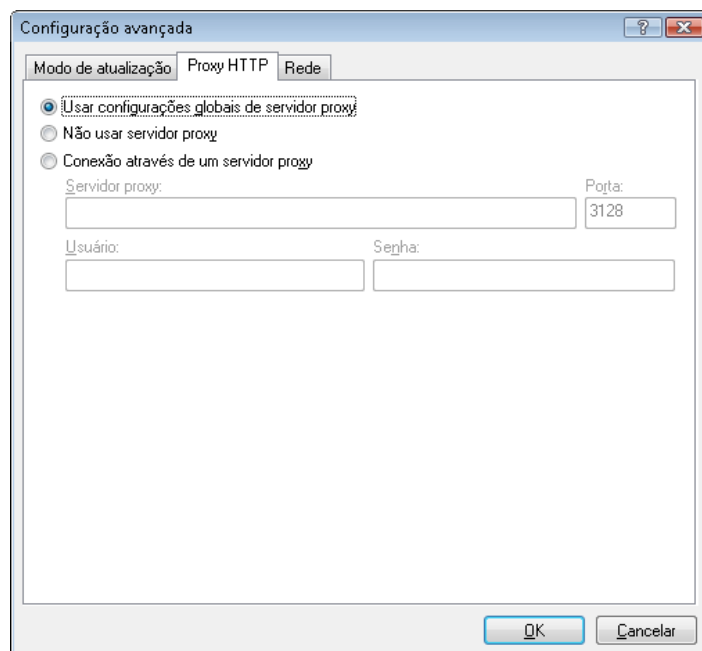
- **Nunca reiniciar o computador**
- **Sugerir opção de reiniciar o computador, se necessário**
- **Se necessário, reinicie o computador sem notificação**

A opção padrão para reiniciar é **Sugerir opção de reiniciar o computador, se necessário**. A escolha das opções mais apropriadas para as atualizações de componentes do programa na guia **Modo de atualização** depende de cada estação de trabalho individual, uma vez que é onde essas configurações serão aplicadas. Esteja ciente de que há diferenças entre estações de trabalho e servidores; por exemplo, reiniciar o servidor automaticamente após uma atualização de programa pode provocar sérios danos.

4.4.1.2.2 Servidor proxy

Para acessar as opções de configuração do servidor proxy para um determinado perfil de atualização: Clique em **Atualizar**, na árvore Configuração avançada (F5) e, em seguida, clique no botão **Configuração...**, à direita de **Configuração avançada de atualização.** Clique na guia **Proxy HTTP** e selecione uma das três opções a seguir:

- **Usar configurações globais de servidor proxy**
- **Não usar servidor proxy**
- **Conexão através de um servidor proxy** (conexão definida pelas propriedades de conexão)

A seleção da opção **Usar configurações globais de servidor proxy** utilizará as opções de configuração do servidor proxy já especificadas dentro da ramificação **Diversos > Servidor proxy** da árvore Configuração avançada.

Selecione a opção **Não usar servidor proxy** para definir explicitamente que nenhum servidor proxy será utilizado para atualizar o ESET Smart Security.

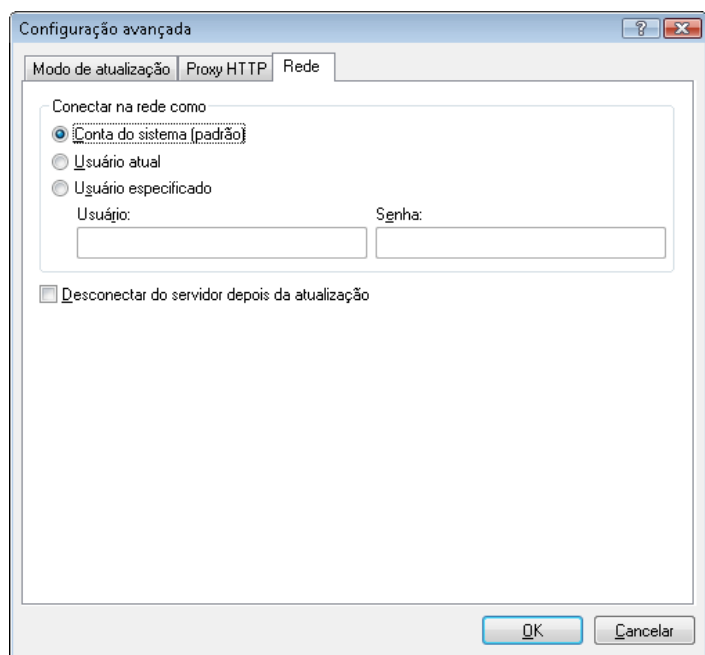
A opção **Conexão através de um servidor proxy** deve ser escolhida se um servidor proxy for utilizado para atualizar o ESET Smart Security e for diferente do servidor proxy especificado nas configurações globais (**Diversos > Servidor proxy**). Nesse caso, as configurações devem ser especificadas aqui: endereço do **Servidor proxy**, **Porta** de comunicação, além de **Nome de usuário** e **Senha** para o servidor proxy, se necessário.

Essa opção deve ser selecionada também se as configurações do servidor proxy não foram configuradas globalmente, mas o ESET Smart Security se conectará a um servidor proxy para obter atualizações.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

4.4.1.2.3 Conexão à rede local

Ao atualizar a partir de um servidor local com um sistema operacional baseado em NT, a autenticação para cada conexão de rede é necessária por padrão. Na maioria dos casos, uma conta do sistema local não tem direitos de acesso suficientes para a pasta Imagem, que contém cópias dos arquivos de atualização. Se esse for o caso, digite o nome de usuário e a senha na seção de configuração da atualização ou especifique uma conta existente na qual o programa acessará o servidor de atualização (Imagem).

Para configurar essa conta, clique na guia **Rede local**. A seção **Conectar à rede local como** apresenta as opções **Conta do sistema (padrão)**, **Usuário atual** e **Usuário especificado**.

Selecione a opção **Conta do sistema** para utilizar a conta do sistema para autenticação. Normalmente, nenhum processo de autenticação ocorrerá se não houver nenhum dado de autenticação fornecido na seção principal de configuração de atualização.

Para garantir que o programa autorize a si próprio utilizando uma conta de usuário atualmente conectada, selecione **Usuário atual** A desvantagem dessa solução é que o programa não é capaz de se conectar ao servidor de atualização se nenhum usuário tiver conectado no momento.

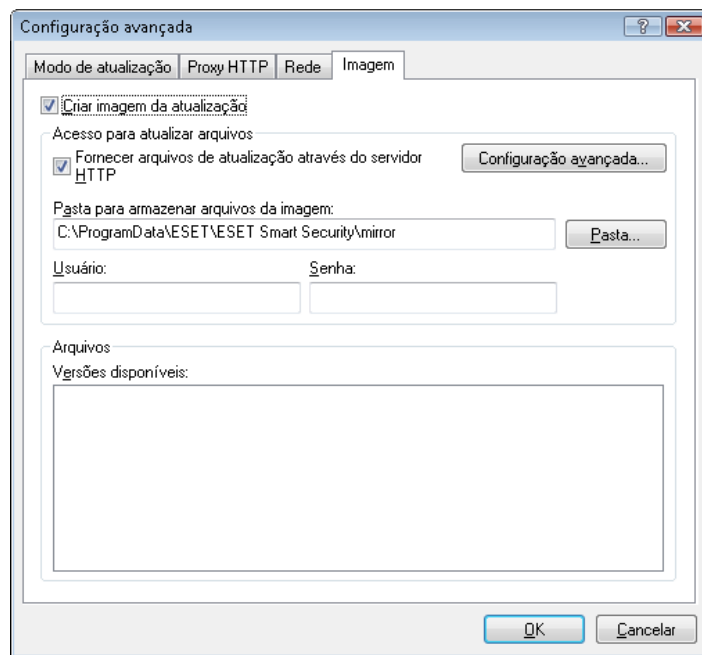
Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação.

A opção padrão para a conexão à rede local é **Conta do sistema**.

Aviso:
Quando a opção **Usuário atual** ou **Usuário especificado** estiver ativada, poderá ocorrer um erro ao alterar a identidade do programa para o usuário desejado. Por isso recomendamos a inserção de dados de autenticação na rede local, na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: nome_domínio\usuário (se for um grupo de trabalho, digite o nome_grupo trabalho\nome) e a senha do usuário. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação é necessária.

4.4.1.2.4 Criação de cópias de atualização – Imagem

O ESET Smart Security Business Edition permite que o usuário crie cópias de arquivos de atualização, que podem ser utilizadas para atualizar outras estações de trabalho localizadas na rede. A atualização das estações de trabalho cliente a partir de uma Imagem otimiza o equilíbrio de carga da rede e economiza a largura de banda da conexão com a Internet.

As opções de configuração para a Imagem do servidor local podem ser acessadas (depois de adicionar uma chave de licença no gerenciador de licenças, localizado na seção Configuração avançada do ESET NOD32 Antivírus Business Edition) na seção **Configuração avançada de atualização:** (para acessar essa seção, pressione F5 e clique em **Atualizar**, na árvore Configuração avançada. Clique no botão **Configuração...**, ao lado da opção **Configuração avançada de atualização:** e selecione a guia **Imagem**).

A primeira etapa na configuração da Imagem é marcar a caixa de seleção **Criar imagem da atualização**. A seleção dessa opção ativa as outras opções de configuração da Imagem, como o modo em que os arquivos serão acessados e o caminho de atualização para os arquivos da imagem.

Os métodos de ativação da Imagem são descritos em detalhes no próximo capítulo, "Variantes de acesso à Imagem". Por enquanto, observe que há duas variantes básicas de acesso à Imagem: a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou através de um servidor HTTP.

A pasta dedicada a armazenar os arquivos de atualização para a Imagem é definida na seção **Pasta para armazenar arquivos da imagem**. Clique em **Pasta...** para procurar uma pasta desejada no computador local ou uma pasta de rede compartilhada. Se a autorização para a pasta especificada for necessária, os dados de autenticação devem ser fornecidos nos campos **Nome de usuário** e **Senha**. O Nome de usuário e a Senha devem ser digitados no formato *Domínio/Usuário* ou *Grupo de trabalho/Usuário*. Lembre-se de fornecer as senhas correspondentes.

Ao especificar a configuração da Imagem detalhada, você pode também especificar as versões de idioma dos quais deseja fazer download das cópias de atualização. A configuração da versão de idioma pode ser acessada na seção **Arquivos > Versões disponíveis:**.

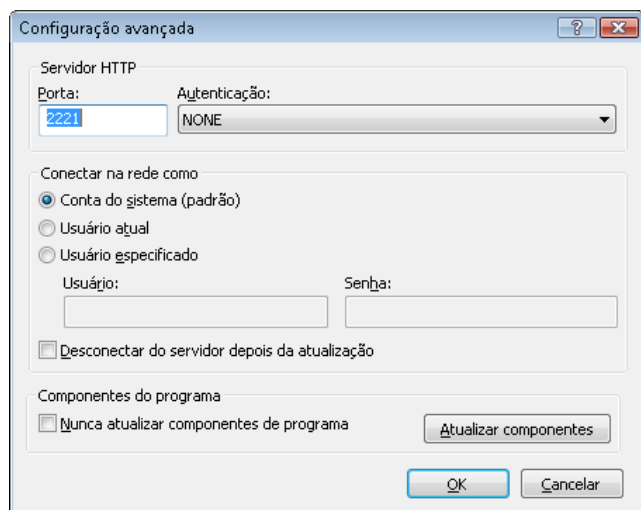
4.4.1.2.4.1 Atualização através da Imagem

Há dois métodos básicos de configuração da Imagem: a pasta com os arquivos de atualização pode ser apresentada como a Imagem como uma pasta de rede compartilhada ou a Imagem como um servidor HTTP.

Acesso à Imagem utilizando um servidor HTTP interno

Essa configuração é a padrão, especificada na configuração de programa predefinida. Para permitir acesso à Imagem utilizando um servidor HTTP, navegue até **Configuração avançada de atualização** (a guia **Imagem**) e selecione a opção **Criar imagem da atualização**.

Na seção **Configuração avançada** da guia **Imagem**, você pode especificar a **Porta do servidor** em que o servidor HTTP escutará, bem como o tipo de **Autenticação** utilizada pelo servidor HTTP. Por padrão, a Porta do servidor é configurada com o valor **2221**.
A opção **Autenticação** define o método de autenticação utilizado para acessar os arquivos de atualização. As seguintes opções estão disponíveis: **NENHUM, Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação básica de nome de usuário e senha. A opção **NTLM** fornece codificação com um método de codificação seguro. Para autenticação, é utilizado o usuário criado na estação de trabalho que compartilha os arquivos de atualização. A configuração padrão é **NENHUM**, que garante acesso aos arquivos de atualização sem a necessidade de autenticação.

Aviso:
Se deseja permitir acesso aos arquivos de atualização por meio do servidor HTTP, a pasta Imagem deve estar localizada no mesmo computador que a instância do ESET Smart Security que os criou.

Depois de concluir a configuração da Imagem, vá até às estações de trabalho e adicione um novo servidor de atualização no formato **http://endereço_IP_do_seu_servidor:2221**. Para fazer isso, siga as etapas abaixo:

- Abra a **Configuração avançada do ESET Smart Security** e clique na ramificação **Atualizar**.
- Clique em **Editar…**, à direita do menu suspenso **Atualizar servidor** e adicione um novo servidor utilizando o seguinte formato: http://endereço_IP_do_seu_servidor:2221
- Selecione esse servidor recém-adicionado à lista de servidores de atualização.

Acesso à Imagem por meio de compartilhamentos de sistema

Primeiro, uma pasta compartilhada deve ser criada em um local ou em um dispositivo de rede. Ao criar a pasta para a Imagem, é necessário fornecer as permissões de "gravação" para o usuário que salvará os arquivos de atualização na pasta e acesso "leitura" para todos os usuários que atualizarão o ESET Smart Security na pasta Imagem.

A seguir, configure o acesso à Imagem na seção **Configuração avançada da atualização** (a guia **Imagem**) desativando a opção **Fornecer arquivos de atualização através do servidor HTTP**. Essa opção está ativada por padrão no pacote de instalação do programa.

Se a pasta compartilhada estiver localizada em outro computador da rede, é necessário especificar os dados de autenticação para acessar o outro computador. Para especificar os dados de autenticação, abra a Configuração avançada do ESET Smart Security (F5) e clique na ramificação **Atualizar**. Clique no botão **Configuração...** e, em seguida, na guia **Rede local**. Essa configuração é a mesma para a atualização, conforme descrito no capítulo "Conexão à rede local".

Depois de concluir a configuração da Imagem, prossiga até as estações de trabalho e configure \\UNC\PATH como o servidor de atualização. Essa operação pode ser concluída utilizando as seguintes etapas:

- Abra a Configuração avançada do ESET Smart Security e clique em **Atualizar**
- Clique em **Editar…**, ao lado da opção Atualizar servidor e adicione um novo servidor utilizando o formato \\UNC\PATH.
- Selecione esse servidor recém-adicionado à lista de servidores de atualização.

OBSERVAÇÃO:
Para obter um funcionamento adequado, o caminho para a pasta Imagem deve ser especificado como um caminho UNC. A atualização de unidades mapeadas pode não funcionar.

4.4.1.2.4.2 Solução de problemas de atualização da Imagem

Dependendo do método de acesso à pasta Imagem, vários tipos de problemas podem ocorrer. Na maioria dos casos, os problemas que ocorrem durante uma atualização do servidor de Imagem são provocados por um ou mais dos seguintes itens: especificação incorreta das opções da pasta Imagem, dados de autenticação incorretos para a pasta Imagem, configuração incorreta nas estações de trabalho locais que tentam fazer download de arquivos de atualização da Imagem ou por uma combinação das razões mencionadas acima. Aqui é fornecida uma visão geral dos problemas mais frequentes que podem ocorrer durante uma atualização da Imagem:

- **O ESET Smart Security relata um erro ao conectar a um servidor de imagem** – provavelmente provocado pela especificação incorreta do servidor de atualização (caminho de rede para a pasta Imagem), a partir do qual as estações de trabalho locais fazem download de atualizações. Para verificar a pasta, clique no **menu Iniciar** do Windows, clique em **Executar**, digite o nome da pasta e clique em **OK**. O conteúdo da pasta deve ser exibido.
- **O ESET Smart Security exige um nome de usuário e uma senha** – provavelmente provocado pela entrada incorreta de dados de autenticação (Nome do usuário e Senha) na seção de atualização. O Nome de usuário e a Senha são utilizados para garantir acesso ao servidor de atualização, a partir do qual o programa atualizará a si próprio. Verifique se os dados de autenticação estão corretos e digitados no formato correto. Por exemplo, *Domínio/Nome de usuário* ou *Grupo de trabalho/Nome de usuário*, além das Senhas correspondentes. Se o servidor da Imagem puder ser acessado por "Todos", esteja ciente de que isso não significa que o acesso é garantido a qualquer usuário. "Todos" não significa qualquer usuário não autorizado; significa apenas que a pasta pode ser acessada por todos os usuários do domínio. Como resultado, se a pasta for acessível a "Todos", um nome de usuário de domínio e uma senha ainda precisarão ser digitados na seção de configuração da atualização.
- **O ESET Smart Security relata um erro ao conectar a um servidor de imagem** – a comunicação na porta definida para acessar a versão HTTP da Imagem está bloqueada.

4.4.2 Como criar tarefas de atualização

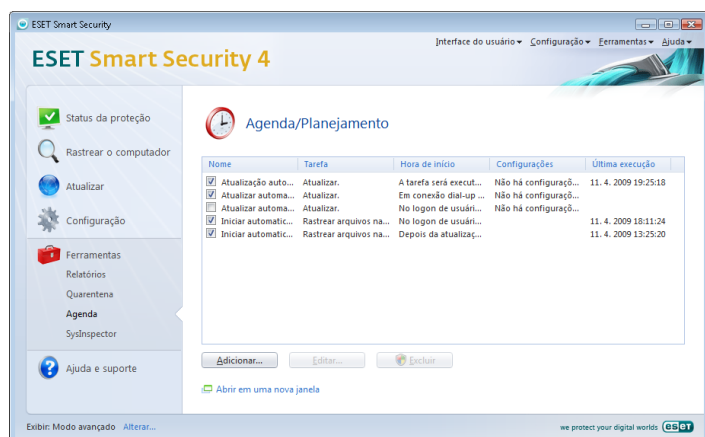
As atualizações podem ser acionadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela de informações exibida depois de clicar em **Atualizar** no menu principal**.**

As atualizações podem também ser executadas como tarefas agendadas – Para configurar uma tarefa agendada, clique em **Ferramentas > Agenda**. Por padrão, as seguintes tarefas são ativadas no ESET Smart Security:

- **Atualização automática de rotina**
- **Atualizar automaticamente após a conexão dial-up**
- **Atualizar automaticamente após logon do usuário**

Cada uma das tarefas de atualização mencionadas pode ser modificada para atender às necessidades do usuário. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte o capítulo "Agenda".

4.5 Agenda

A Agenda estará disponível se o Modo avançado no ESET Smart Security estiver ativado. A **Agenda** pode ser encontrada no menu principal do ESET Smart Security em **Ferramentas**. A Agenda contém uma lista resumida de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidos e o perfil de rastreamento utilizado.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Atualização automática de rotina**
- **Atualizar automaticamente após a conexão dial-up**
- **Atualizar automaticamente após logon do usuário**
- **Verificação de arquivo na inicialização automática após logon do usuário**
- **Verificação de arquivo na inicialização automática após atualização bem-sucedida do banco de dados de assinatura de vírus**

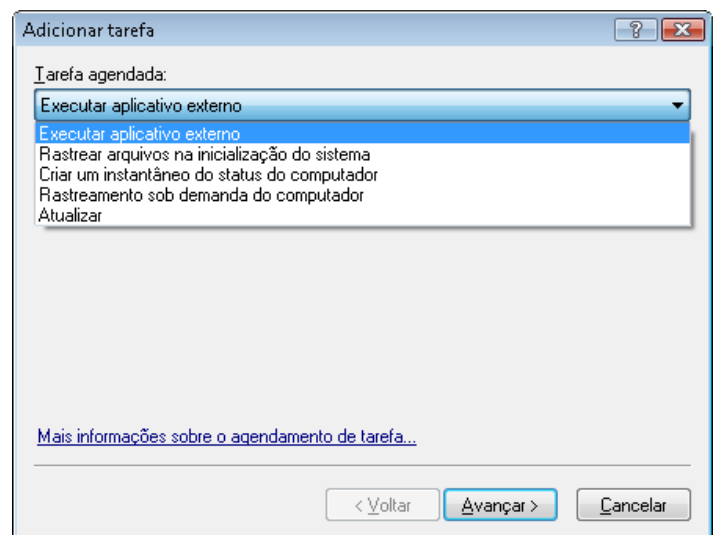
Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificar e clique no botão **Editar...**

4.5.1 Finalidade do agendamento de tarefas

A Agenda gerencia e inicia tarefas agendadas com a configuração e as propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e a hora, bem como os perfis especificados para serem utilizados durante a execução da tarefa.

4.5.2 Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique no botão **Adicionar...** ou clique com o botão direito do mouse e selecione **Adicionar...** no menu de contexto. Há cinco tipos de tarefas agendadas disponíveis:

- **Executar aplicativo externo**
- **Manutenção de relatórios**
- **Verificação de arquivo na inicialização do sistema**
- **Rastreamento sob demanda do computador**
- **Atualizar**

Como **Rastreamento sob demanda do computador** e **Atualizar** são as tarefas agendadas utilizadas com mais frequência, explicaremos como adicionar uma nova tarefa de atualização.

No menu suspenso **Tarefa agendada:**, selecione **Atualizar**. Clique em **Avançar** e digite o nome da tarefa no campo **Nome da tarefa:**. Selecione a frequência da tarefa. As seguintes opções estão disponíveis: **Uma vez, Repetidamente, Diariamente**, **Semanalmente** e **Acionado por evento**. Com base na frequência selecionada, diferentes parâmetros de atualização serão exibidos para você. A seguir, defina a ação a ser tomada se a tarefa não puder ser executada ou concluída na hora agendada. As três opções a seguir estão disponíveis:

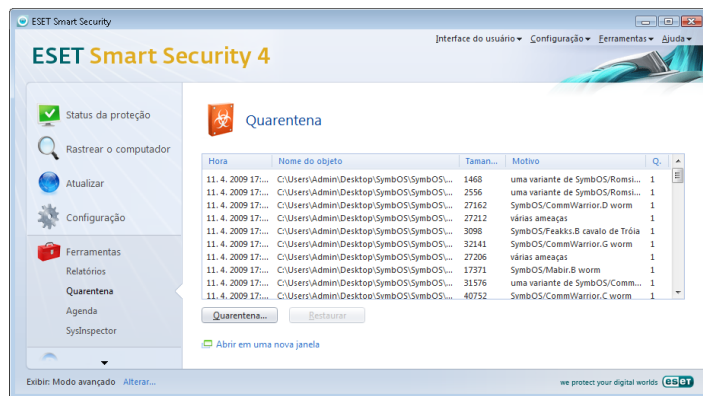
- **Aguardar até a próxima hora agendada**
- **Executar a tarefa tão logo quanto possível**
- **Executar a tarefa imediatamente se a hora desde a última execução exceder o intervalo especificado** (o intervalo pode ser definido imediatamente utilizando a caixa de rolagem **Intervalo da tarefa**)

Na próxima etapa, uma janela resumida com informações sobre a tarefa agendada atual será exibida; a opção **Executar a tarefa com parâmetros específicos** deverá ser ativada automaticamente. Clique no botão **Finalizar**.

Uma janela de diálogo aparecerá permitindo selecionar perfis a serem utilizados para a tarefa agendada. Aqui você pode especificar um perfil primário e alternativo, que é utilizado caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em **OK** na janela **Atualizar perfis**. A nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

4.6 Quarentena

A principal tarefa da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Smart Security.

O usuário pode optar por colocar em quarentena qualquer arquivo que desejar. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo rastreador antivírus. Os arquivos colocados em quarentena podem ser enviados aos laboratórios da ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (**adicionada pelo usuário...**) e o número de ameaças (por exemplo, se ele for um arquivo que contém múltiplas ameaças).

4.6.1 Arquivos em quarentena

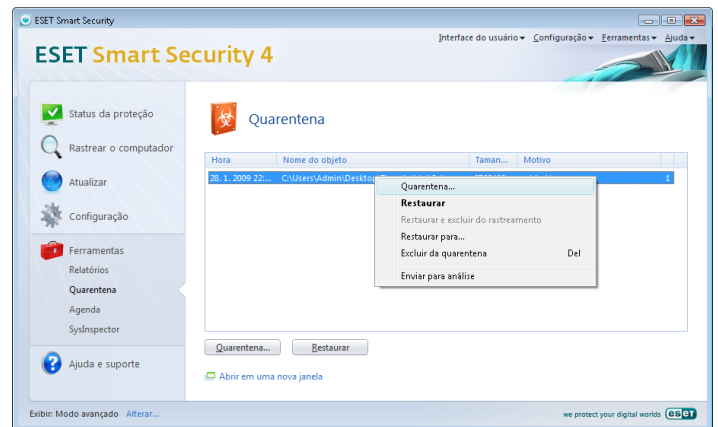
O programa coloca automaticamente os arquivos excluídos em quarentena (se você não cancelou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando no botão **Quarentena...** Se esse for o caso, o arquivo original não será removido do seu local original. O menu de contexto pode ser utilizado também para essa finalidade; clique com o botão direito do mouse na janela de quarentena e selecione **Adicionar...**

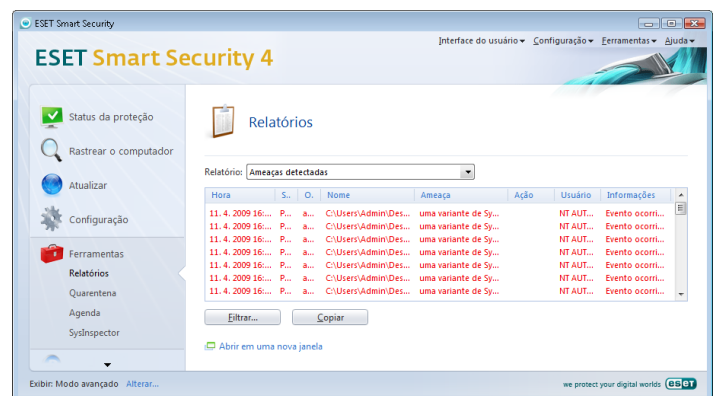
4.6.2 Restauração da quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Utilize o recurso **Restaurar** para essa finalidade; esse recurso está disponível no menu de contexto clicando com o botão direito do mouse em um arquivo específico, na janela de quarentena. O menu de contexto oferece também a opção **Restaurar para**, que permite que o usuário restaure um arquivo para um local diferente do local original do qual ele foi excluído.

OBSERVAÇÃO:
Se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do rastreamento depois de restaurá-lo e envie-o para o Atendimento ao cliente da ESET.

4.6.3 Envio de arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi avaliado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o laboratório da ESET. Para enviar um arquivo diretamente da janela de quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

4.7 Relatórios

Os Relatórios contêm informações sobre todos os eventos importantes do programa que podem ter ocorrido e fornece uma visão geral das ameaças detectadas. Os Relatórios atuam como uma ferramenta essencial na análise do sistema, na detecção de ameaças e na solução de problemas. Os Relatórios são realizados ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento do relatório. É possível exibir mensagens de texto e relatórios diretamente do ambiente do ESET Smart Security, bem como arquivar os relatórios.

Os relatórios podem ser acessados na janela principal do ESET Smart Security clicando em **Ferramentas > Relatórios**. Selecione o tipo de relatório utilizando o menu suspenso **Relatório:** na parte superior da janela. Os seguintes relatórios estão disponíveis:

1. **Ameaças detectadas** – Use essa opção para exibir todas as informações sobre eventos relacionados à detecção de ameaças.

2. **Eventos** – Essa opção foi desenvolvida para solucionar problemas de administradores e usuários do sistema. Todas as ações importantes executadas pelo ESET Smart Security são registradas nos Relatórios de eventos.

3. **Rastreamento sob demanda do computador scan** – Os resultados de todos os rastreamentos concluídos são exibidos nessa janela. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo Rastreamento sob demanda.

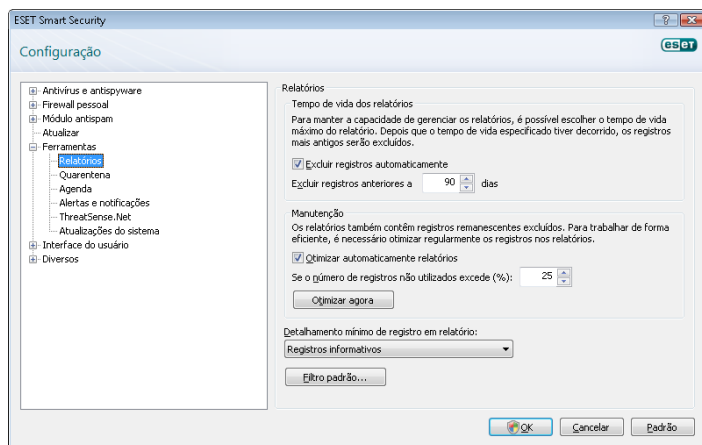
4. **Relatório do Firewall pessoal da ESET** – Contém os registros de

todos os fatos detectados pelo Firewall pessoal e relacionados a ele. A análise do relatório do firewall pode ajudar a detectar as tentativas de infiltração no sistema a tempo de evitar o acesso não autorizado ao seu sistema.

Em cada seção, as informações exibidas podem ser copiadas diretamente para a área de transferência, selecionando a entrada e clicando no botão **Copiar** Para selecionar múltiplas entradas, podem ser usadas as teclas CTRL e SHIFT.

4.7.1 Manutenção de relatórios

A configuração de Relatórios do ESET Smart Security é acessível a partir da janela principal do programa. Clique na árvore **Configuração > Entrar na configuração avançada... > Ferramentas > Relatórios**. Você pode especificar as seguintes opções para relatórios:

- **Excluir registros automaticamente:** As entradas de relatório mais antigas do que o número de dias especificado são automaticamente excluídas
- **Otimizar relatórios automaticamente**: Permite a desfragmentação automática dos relatórios se o percentual especificado de registros não utilizados foi excedido
- **Detalhamento mínimo do relatório:** Especifica o nível de detalhamento do relatório. Opções disponíveis:
  - **Erros críticos** – Registra em relatório apenas erros críticos (erro ao iniciar a Proteção antivírus, Firewall pessoal, etc...)
  - **Erros** – Apenas as mensagens "Erro ao fazer download de arquivo" são registradas, além dos erros críticos
  - **Avisos** – Registra erros críticos e mensagens de aviso
  - **Registros informativos** – Registra as mensagens informativas, incluindo as mensagens de atualização bem-sucedida e todos os registros acima
  - **Registros de diagnóstico** – Relata informações necessárias para o ajuste otimizado do programa e de todos os registros acima

4.8 Interface do usuário

As opções de configuração da interface do usuário no ESET Smart Security podem ser modificadas para que você possa adaptar o ambiente de trabalho conforme suas necessidades. Essas opções de configuração podem ser acessadas na ramificação **Interface do usuário** da árvore Configuração avançada do ESET Smart Security.

A seção **Elementos da interface do usuário** proporciona aos usuários a capacidade de alternar para o Modo avançado, se desejar. O modo Avançado exibe configurações mais detalhadas e controles adicionais para o ESET Smart Security.

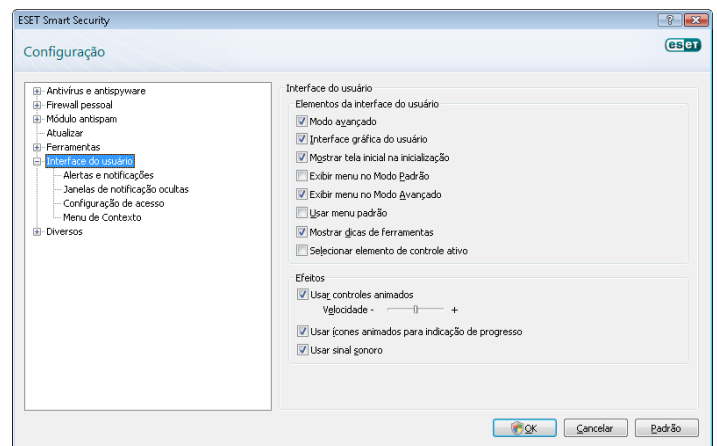
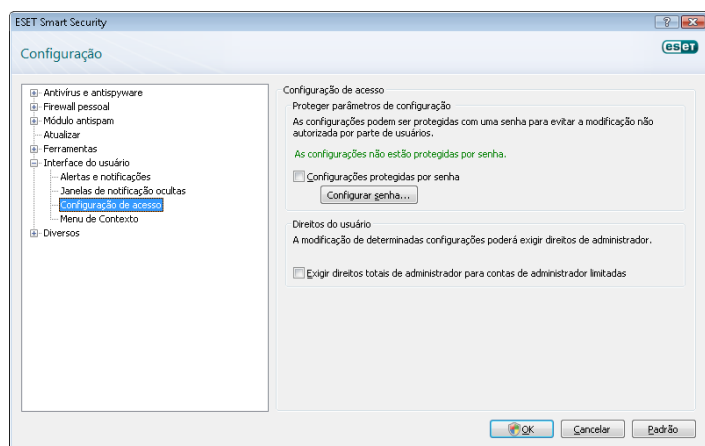
A opção **Interface gráfica do usuário** deve ser desativada se os elementos gráficos reduzirem o desempenho do computador ou provocarem outros problemas. A interface gráfica pode também ser desativada para usuários com deficiência visual, uma vez que pode causar conflito com aplicativos especiais utilizados para leitura do texto exibido na tela.

Se desejar desativar a tela inicial do ESET Smart Security, desative a opção **Mostrar tela inicial na inicialização**.

Na parte superior da janela principal do programa ESET Smart Security, há um menu Padrão que pode ser ativado ou desativado com base na opção **Usar menu padrão**.

Se a opção **Mostrar dicas de ferramentas** estiver ativada, uma breve descrição de qualquer opção será exibida se o cursor do mouse for colocado sobre a opção desejada. A opção **Selecionar elemento de controle ativo** fará com que o sistema destaque qualquer elemento que esteja atualmente na área ativa do cursor do mouse. O elemento destacado será ativado após um clique do mouse.

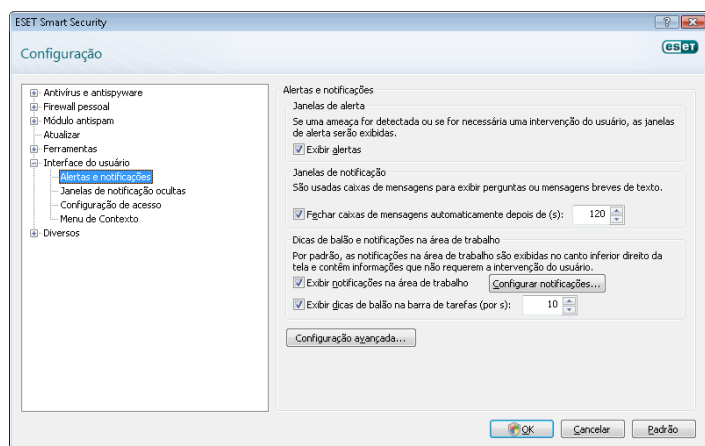
Para reduzir ou aumentar a velocidade dos efeitos animados, selecione a opção **Usar controles animados** e mova o controle deslizante **Velocidade** para a esquerda ou para a direita.

Para ativar o uso de ícones animados, a fim de exibir o andamento de diversas operações, marque a caixa de seleção **Usar ícones animados...** Se desejar que o programa emita um aviso sonoro se ocorrer um evento importante, selecione a opção **Usar sinal sonoro**.

Os recursos da **Interface do usuário** também incluem a opção para proteger por senha os parâmetros de configuração do ESET Smart Security. Essa opção está localizada no submenu **Proteção de configurações** em **Interface do usuário**. Para fornecer segurança máxima ao seu sistema, é fundamental que o programa seja configurado corretamente. Modificações não autorizadas podem resultar na perda de dados importantes. Para configurar uma senha para proteger os parâmetros de configuração, clique em **Digitar senha...**

4.8.1 Alertas e notificações

A seção **Configuração de alertas e notificações** em **Interface do usuário** permite configurar como os alertas e as notificações do sistema são tratados no ESET Smart Security 4.

O primeiro item é **Exibir alertas**. A desativação dessa opção cancelará todas as janelas de alerta e é adequada apenas para uma quantidade limitada de situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

Para fechar as janelas pop-up automaticamente após um determinado período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente após (s):**. Se não forem fechadas manualmente pelo usuário, as janelas de alerta serão fechadas automaticamente após o período de tempo especificado ter expirado.

As notificações na área de trabalho e as dicas de balão são apenas informativas e não fornecem nem exigem interação com o usuário. Elas são exibidas na área de notificação, no canto inferior direito da tela. Para ativar a exibição de notificações na área de trabalho, selecione a opção **Exibir notificações na área de trabalho**. Opções mais detalhadas – o tempo de exibição e a transparência da janela de notificação podem ser modificados clicando no botão **Configurar notificações...** Para visualizar o comportamento de notificações, clique no botão **Visualizar**. Para configurar a duração do tempo de exibição das dicas de balão, consulte a opção **Exibir dicas de balão na barra de tarefas (por s)**.

Clique em **Configuração avançada...** para inserir opções de configuração adicionais de **Alertas e notificações** que incluem a opção **Exibir somente notificações que exijam interação do usuário**. Essa opção permite ativar/desativar a exibição de alertas e notificações que não exijam interação do usuário. Selecione a opção Exibir somente notificações que exijam interação do usuário ao executar aplicativos em modo de tela inteira para omitir todas as notificações não interativas. No menu suspenso Detalhamento mínimo de eventos a serem exibidos, é possível selecionar o nível de gravidade inicial de alertas e notificações a serem exibidos.

O último recurso desta seção é a especificação de endereços de notificações em um ambiente com múltiplos usuários. O campo **Em sistemas com múltiplos usuários, exibir as notificações na tela do usuário:** permite que o usuário defina quem receberá notificações importantes do ESET Smart Security 4. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Essa opção é especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

4.9 ThreatSense.Net

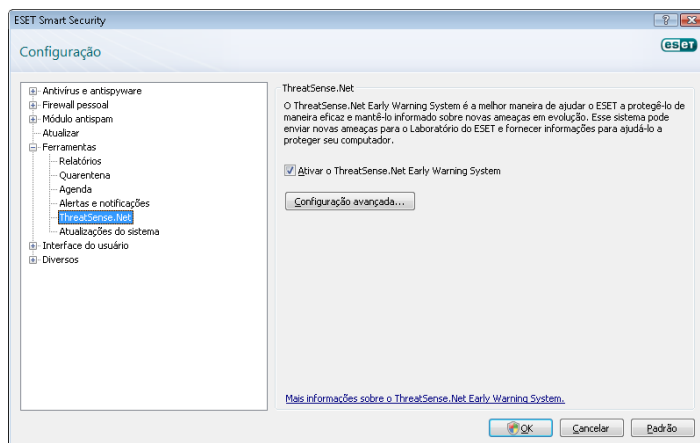
O ThreatSense.Net Early Warning System é uma ferramenta que mantém a ESET contínua e imediatamente informada sobre novas ameaças. O sistema de alerta bidirecional do ThreatSense.Net Early Warning System tem uma única finalidade: melhorar a proteção que podemos lhe proporcionar. A melhor maneira de garantir que vemos novas ameaças assim que elas aparecem é fazermos "link" com o máximo possível de nossos clientes e usá-los como nossos Sentinelas de ameaças. Há duas opções:

1. Você pode optar por não ativar o ThreatSense.Net Early Warning System. Você não perderá nenhuma funcionalidade do software e receberá a melhor proteção que podemos proporcionar.

2. Você pode configurar o Early Warning System (Sistema de alarme antecipado) para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido, em único arquivo. Esse arquivo pode ser enviado para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar suas capacidades de detecção de ameaças. O ThreatSense.Net Early Warning System coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, informações sobre a data e a hora, o processo pelo qual a ameaça apareceu no seu computador e informações sobre o sistema operacional do seu computador. Algumas dessas informações podem incluir informações pessoais sobre o usuário do computador, como nomes de usuários em um caminho de diretório, etc.

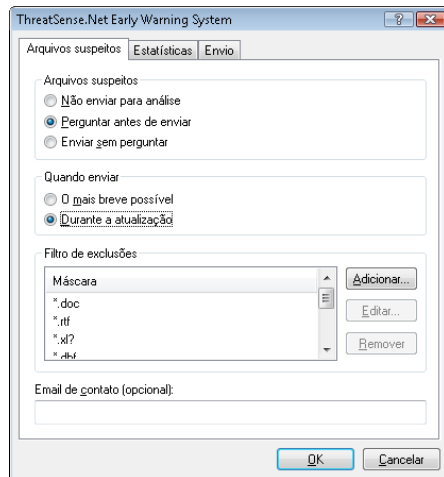
Caso haja alguma possibilidade de que isso possa revelar ocasionalmente algumas informações sobre você ou seu computador para o nosso laboratório de ameaças na ESET, essas informações não serão utilizadas para QUALQUER outra finalidade, exceto nos ajudar a reagir imediatamente contra novas ameaças.

Por padrão, o ESET Smart Security é configurado para perguntar antes de enviar arquivos suspeitos ao laboratório de ameaças da ESET para análise detalhada. Deve-se observar que arquivos com determinadas extensões, como, por exemplo, .doc ou .xls, são sempre excluídos do envio se uma ameaça for detectada neles. Você pode também adicionar outras extensões se houver arquivos específicos cujo envio você ou sua empresa desejam impedir.

A configuração do ThreatSense.Net pode ser acessada na árvore Configuração avançada, em **Ferramentas > ThreatSense.Net**. Marque a caixa de seleção **Ativar o ThreatSense.Net Early Warning System**. Essa ação permite que você o ative. Em seguida, clique no botão **Configuração avançada...**

4.9.1 Arquivos suspeitos

A guia **Arquivos suspeitos** permite configurar a maneira como as ameaças serão enviadas ao laboratório da ESET para análise.

Se você encontrou um arquivo suspeito, poderá enviá-lo ao nosso laboratório de vírus para análise. Se for confirmado que o aplicativo é malicioso, sua detecção será adicionada à próxima atualização de assinatura de vírus.

O envio de arquivos pode ser configurado para ser executado automaticamente sem perguntar. Se essa opção estiver selecionada, os arquivos suspeitos serão enviados no segundo plano. Se desejar saber quais arquivos foram enviados para análise e confirmar o envio, selecione a opção **Perguntar antes de enviar**.

Se não desejar que os arquivos sejam enviados, selecione **Não enviar para análise**. Observe que o não envio de arquivos para análise não afeta o envio de informações estatísticas para a ESET. As informações estatísticas estão configuradas em sua própria seção de configuração, descrita no próximo capítulo.

Quando enviar
Os arquivos suspeitos serão enviados aos laboratórios da ESET para análise o mais breve possível. Essa é a opção recomendada se uma conexão permanente com a Internet estiver disponível e os arquivos suspeitos puderem ser enviados sem atraso. A outra opção é enviar arquivos suspeitos **Durante a atualização**. Se essa opção estiver selecionada, os arquivos suspeitos serão coletados e o upload deles será feito para os servidores do Early Warning System durante uma atualização.

Filtro de exclusões
Nem todos os arquivos têm de ser enviados para análise. O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Por exemplo, pode ser útil excluir arquivos que podem ter informações potencialmente sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (Microsoft Office, OpenOffice). A lista de arquivos excluídos pode ser ampliada, se desejar.

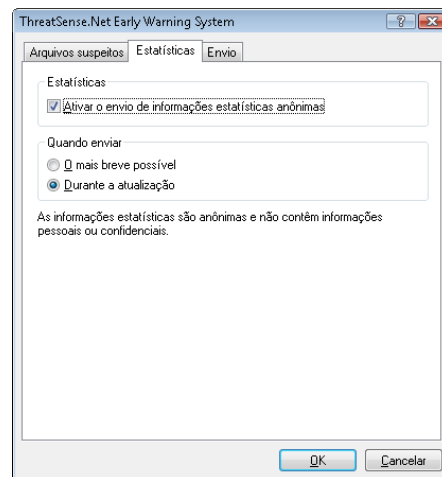
Email de contato
O email de contato é enviado à ESET junto com os arquivos suspeitos e pode ser usado para entrar em contato com você se precisarmos de mais informações sobre os arquivos enviados para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

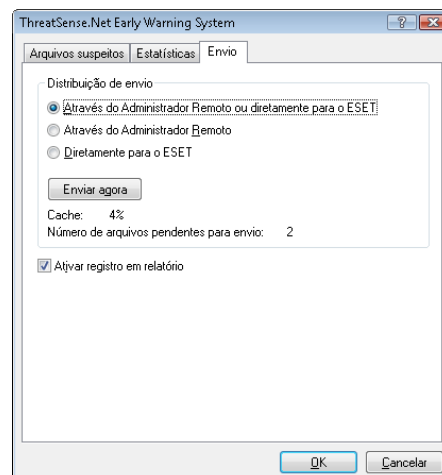
4.9.2 Estatísticas

O ThreatSense.Net Early Warning System coleta informações anônimas sobre o seu computador que estejam relacionadas a ameaças recém-detectadas. Essas informações podem incluir o nome da ameaça, a data e a hora em que ela foi detectada, a versão do ESET Smart Security, a versão do sistema operacional do computador e a configuração de local. As estatísticas são normalmente enviadas para os servidores da ESET uma ou duas vezes por dia.

Um exemplo de um pacote estatístico enviado:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

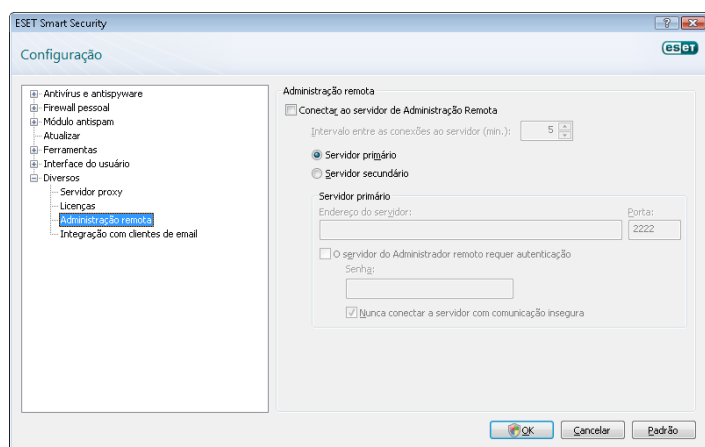
Quando enviar
Na seção **Quando enviar**, é possível definir quando as informações estatísticas serão enviadas. Se optar por enviar **O mais breve possível**, as informações estatísticas serão enviadas imediatamente após serem criadas. Essa configuração é adequada se uma conexão permanente com a Internet estiver disponível. Se a opção **Durante a atualização** estiver selecionada, informações estatísticas serão mantidas e enviadas em grupo durante a próxima atualização.

4.9.3 Envio

Nesta seção, você pode escolher se os arquivos e informações estatísticas serão enviados usando o Administrador remoto da ESET ou diretamente para a ESET. Se desejar ter certeza de que os arquivos suspeitos e as informações estatísticas serão enviados para a ESET, selecione a opção **Usando o Administrador remoto ou diretamente para a ESET**. Se essa opção estiver selecionada, os arquivos e estatísticas serão enviados usando todos os meios disponíveis. O envio de arquivos suspeitos usando o Administrador remoto envia arquivos e estatísticas para o servidor do administrador remoto, que garantirá o envio posterior para os laboratórios de vírus da ESET. Se a opção **Diretamente para a ESET** estiver marcada, todos os arquivos suspeitos e informações estatísticas serão enviados para o laboratório de vírus da ESET diretamente do programa.

Quando houver arquivos com envio pendente, o botão **Enviar agora** estará ativado nessa janela de configuração. Clique neste botão se desejar enviar os arquivos e informações estatísticas imediatamente.

Marque a opção **Ativar relatório** para ativar o registro de envio de arquivos e de informações estatísticas. Após cada envio de arquivo suspeito ou de uma parte de informações estatísticas, é criada uma entrada no relatório de eventos.

4.10 Administração remota

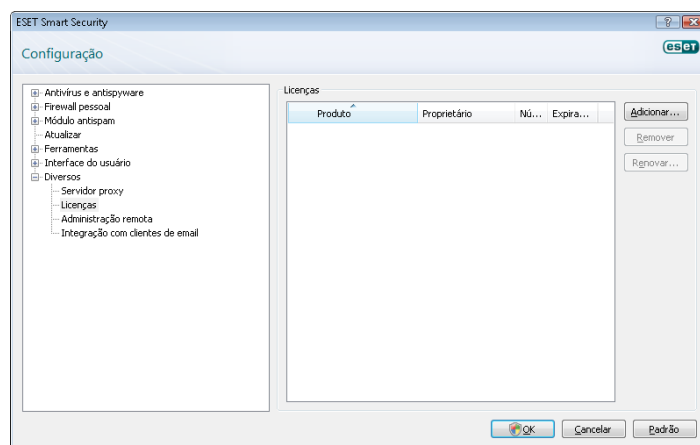
A Administração remota é uma ferramenta poderosa para a manutenção da política de segurança e para a obtenção de uma visão geral do gerenciamento de segurança dentro da rede. É especialmente útil quando aplicada a redes maiores. A Administração Remota não apenas aumenta o nível de segurança, mas fornece também facilidade de uso na administração do ESET Smart Security em estações de trabalho cliente.

As opções de configuração da Administração remota estão disponíveis na janela principal do programa ESET Smart Security. Clique em **Configuração > Entrar na árvore inteira da configuração avançada... > Diversos > Administração remota**.

A janela Configuração permite ativar o modo de administração remota marcando primeiro a caixa de seleção **Conectar ao servidor de Administração remota**. É possível acessar as outras opções descritas a seguir:

- **Endereço do servidor** – Endereço de rede do servidor em que o servidor da administração remota está instalado.
- **Porta** – Esse campo contém uma porta de servidor predefinida utilizada para conexão. Recomendamos que você deixe a configuração de porta predefinida como 2222.
- **Intervalo entre as conexões ao servidor (em min)** – Essa opção designa a frequência em que o ESET Smart Security se conectará ao servidor ERA para enviar dados. Em outras palavras, as informações são enviadas nos intervalos de tempo definidos aqui. Se estiver configurado como 0, as informações serão enviadas a cada 5 segundos.
- **O Administrador remoto exige autenticação** – Permite digitar uma senha para se conectar ao servidor do administrador remoto, se solicitada.

Clique em **OK** para confirmar as alterações e aplicar as configurações. O ESET Smart Security utilizará essas configurações para se conectar ao servidor remoto.

4.11 Licença

A ramificação **Licença** permite gerenciar as chaves de licença do ESET Smart Security e outros produtos da ESET como, por exemplo, o ESET Remote Administrator, o ESET NOD32 para Microsoft Exchange, etc. Após a compra, as chaves de licença são enviadas junto com o seu Nome de usuário e Senha. Para **Adicionar/remover** uma chave de licença, clique no botão correspondente na janela do gerenciador de licenças. O gerenciador de licenças pode ser acessado na árvore Configuração avançada, em **Diversos > Licenças**.

A chave de licença é um arquivo de texto que contém informações sobre o produto adquirido: o proprietário, o número de licenças e a data de expiração.

A janela do gerenciador de licenças permite que o usuário faça upload e visualize o conteúdo de uma chave de licença utilizando o botão **Adicionar**...; as informações contidas são exibidas no gerenciador. Para excluir arquivos de licença da lista, clique em **Remover**.

Se uma chave de licença expirou e você estiver interessado em comprar uma renovação, clique no botão **Solicitar...** – você será redirecionado para a nossa loja on-line.

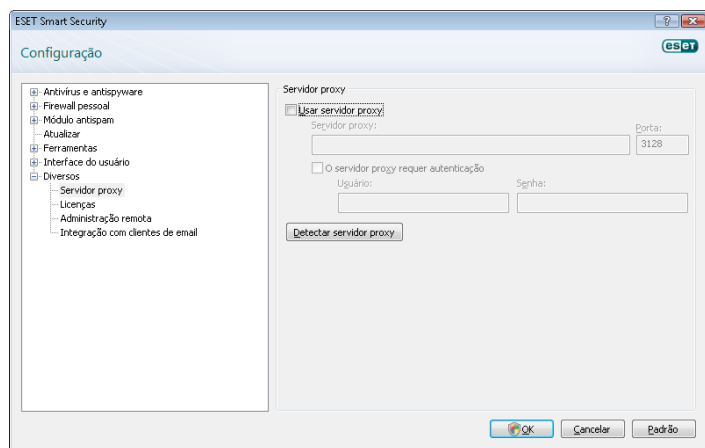
5. Usuário avançado

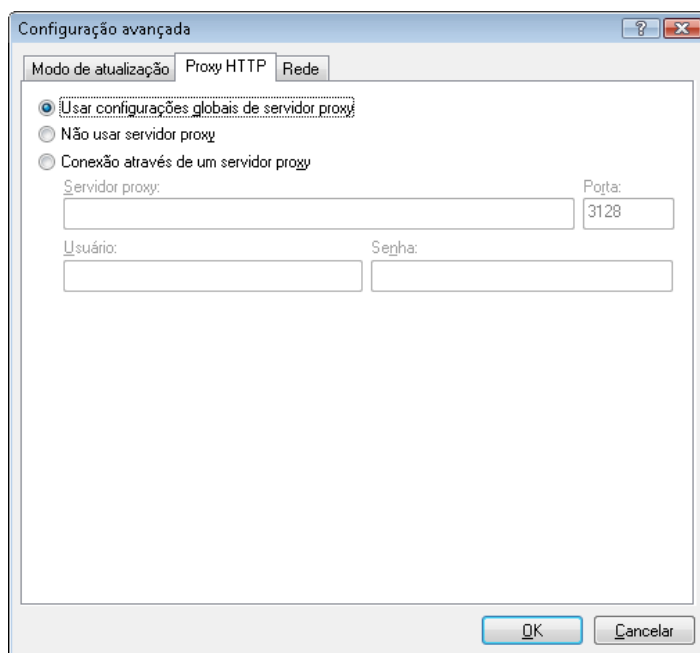
Este capítulo descreve os recursos do ESET Smart Security que podem ser úteis para usuários mais avançados. As opções de configuração desses recursos podem ser acessadas somente no Modo avançado. Para alternar para o Modo avançado, clique em **Alternar para modo avançado** no canto inferior esquerdo da janela principal do programa ou pressione CTRL + M no teclado.

5.1 Configuração do servidor proxy

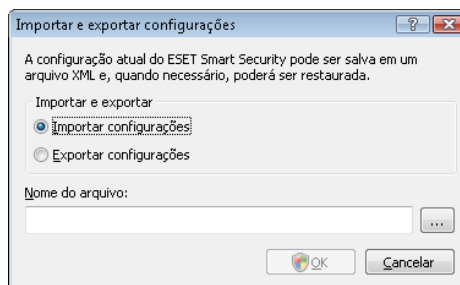
No ESET Smart Security, a configuração do servidor proxy está disponível em duas seções diferentes dentro da estrutura da Configuração avançada.

Primeiro, as configurações do servidor proxy podem ser configuradas em **Diversos > Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET Smart Security. Aqui, os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

Para especificar as configurações do servidor proxy para esse nível, marque a caixa de seleção **Utilizar servidor proxy** e, em seguida, digite o endereço do servidor proxy no campo **Servidor proxy:**, junto com o número da **Porta** do servidor proxy.

Se a comunicação com o servidor proxy exigir autenticação, marque a caixa de seleção **O servidor proxy exige autenticação** e digite um **Nome de usuário** e uma **Senha** válidos nos respectivos campos. Clique no botão **Detectar servidor proxy** para detectar e inserir automaticamente as configurações do servidor proxy. Os parâmetros especificados no Internet Explorer serão copiados. Observe que esse recurso não recupera dados de autenticação (Nome de usuário e Senha); eles devem ser fornecidos pelo usuário.

As configurações do servidor proxy podem ser estabelecidas dentro da **Configuração avançada de atualização** (ramificação **Atualizar** da árvore Configuração avançada). Essa configuração é aplicada ao perfil de atualização fornecido e é recomendada para laptops, uma vez que eles frequentemente recebem atualizações de assinatura de vírus de diferentes locais. Para obter mais informações sobre essa configuração, consulte a Seção 4.4, "Atualização do sistema".

5.2 Exportar/importar configurações

A exportação e a importação da configuração atual do ESET Smart Security está disponível no Modo avançado em **Configuração**.

Tanto a exportação como a importação utilizam o tipo de arquivo .xml. A exportação e a importação são úteis se você precisar fazer backup da configuração atual do ESET Smart Security para poder utilizá-lo posteriormente (por qualquer razão). A opção Exportar configurações também será útil para aqueles que desejam utilizar a configuração favorita do ESET Smart Security em diversos sistemas; eles precisam apenas importar o arquivo .xml.

5.2.1 Exportar configurações

A exportação da configuração é muito fácil. Se desejar salvar a configuração atual do ESET Smart Security, clique em **Configuração > Importar e exportar configurações...** Selecione a opção **Exportar configurações** e digite o nome do arquivo de configuração. Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.

5.2.2 Importar configurações

As etapas para importar uma configuração são muito semelhantes. Selecione novamente **Importar e exportar configurações** e selecione a opção **Importar configurações**. Clique no botão **...** e procure o arquivo de configuração que deseja importar.

5.3 Command Line

O módulo antivírus do ESET Smart Security pode ser iniciado pela linha de comando – manualmente (com o comando "ecls") ou com um arquivo em lotes ("bat").

Os seguintes parâmetros e chaves podem ser utilizados ao executar o scanner sob demanda a partir da linha de comando:

Opções gerais:

– help	mostrar a ajuda e encerrar
– version	mostrar as informações sobre a versão e encerrar
– base-dir = FOLDER	carregar módulos da PASTA
– quar-dir = FOLDER	PASTA de quarentena
– aind	mostrar indicador de atividade

Alvos:

– files	rastrear arquivos (padrão)
– no-files	não rastrear arquivos
– boots	rastrear setores de inicialização (padrão)
– no-boots	não rastrear setores de inicialização
– arch	rastrear arquivos compactados (padrão)
– no-arch	não rastrear arquivos compactados
– max-archive-level = LEVEL	NÍVEL máximo de encadeamento de arquivos
– scan-timeout = LIMIT	rastrear arquivos compactados pelo LIMITE máximo de segundos. Se o tempo de rastreamento atingir esse limite, o rastreamento do arquivo compactado será interrompido e o rastreamento continuará com o próximo arquivo
– max-arch-size=SIZE	rastrear somente os primeiros bytes de TAMANHO nos arquivos compactados (padrão 0 = sem limite)
– mail	rastrear arquivos de email
– no-mail	não rastrear arquivos de email
– sfx	rastrear arquivos compactados de autoextração
– no-sfx	não rastrear arquivos compactados de autoextração
– rtp	rastrear empacotadores em tempo real
– no-rtp	não rastrear empacotadores em tempo real
– exclude = FOLDER	excluir PASTA do rastreamento
– subdir	rastrear subpastas (padrão)
– no-subdir	não rastrear subpastas
– max-subdir-level = LEVEL	NÍVEL máximo de aninhamento de subpastas (padrão 0 = sem limite)
– symlink	seguir links simbólicos (padrão)
– no-symlink	ignorar links simbólicos
– ext-remove = EXTENSIONS	
– ext-exclude = EXTENSIONS	excluir do rastreamento EXTENSÕES, delimitadas por dois pontos

Métodos:

– adware	rastrear se há Adware/Spyware/Riskware
– no-adware	não rastrear se há Adware/Spyware/Riskware
– unsafe	rastrear se há aplicativos potencialmente não seguros
– no-unsafe	não rastrear se há aplicativos potencialmente não seguros
– unwanted	rastrear se há aplicativos potencialmente não desejados
– no- unwanted	não rastrear se há aplicativos potencialmente não desejados
– pattern	usar assinaturas
– no-pattern	não usar assinaturas
– heur	ativar heurística
– no-heur	desativar heurística
– adv-heur	ativar heurística avançada
– no-adv-heur	desativar heurística avançada

Limpeza:

– action = ACTION	executar AÇÃO em objetos infectados. Ações disponíveis: nenhuma, limpar, aviso
– quarantine	copiar os arquivos infectados para Quarentena (completa a AÇÃO)
– no-quarantine	não copiar arquivos infectados para Quarentena

Relatórios:

– log-file=FILE	registrar saída para ARQUIVO
– log-rewrite	substituir arquivo de saída (padrão – anexar)
– log-all	registrar também arquivos limpos
– no-log-all	não registrar arquivos limpos (padrão)

Possíveis códigos de saída do rastreamento:

0	– nenhuma ameaça encontrada
1	– ameaça encontrada, mas não limpa
10	– alguns arquivos infectados restantes
101	– erro no arquivo compactado
102	– erro de acesso
103	– erro interno

OBSERVAÇÃO: Os códigos de saída maiores que 100 significam que o arquivo não foi rastreado e, nesse caso, pode estar infectado.

5.4 ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o seu computador e exibe os dados coletados de uma maneira abrangente. Informações como drivers e aplicativos instalados, conexões de rede ou entradas importantes de registro podem ajudá-lo a investigar o comportamento suspeito do sistema, seja devido à incompatibilidade de software ou de hardware ou à infecção por malware.

É possível encontrar o SysInspector em duas variantes do portfólio da ESET. O aplicativo portátil (SysInspector.exe) pode ser obtido por download gratuitamente no site da ESET. A variante integrada está incluída no ESET Smart Security 4. Para abrir a seção do SysInspector, ative o modo de exibição Avançado no canto inferior esquerdo e clique em **Ferramentas** > **SysInspector**. As duas variantes são idênticas em função e possuem os mesmos controles de programa. A única diferença é o modo como as saídas são gerenciadas. O aplicativo portátil permite exportar instantâneo do sistema para um arquivo XML e salvá-lo em seu disco. Isso é possível também no SysInspector integrado. Além disso, é possível armazenar adequadamente os instantâneos do sistema diretamente em **ESET Smart Security 4** > **Ferramentas** > **SysInspector** (para obter mais informações, consulte 5.4.1.4 SysInspector como parte do ESS).

Aguarde alguns instantes enquanto o ESET SysInspector rastreia o computador. Ele pode levar de 10 segundos a alguns minutos, dependendo da configuração de hardware, do sistema operacional e da quantidade de aplicativos instalados no computador.

5.4.1 Interface do usuário e uso do aplicativo

Para facilitar o uso, a janela principal é dividida em quatro seções – Controles do programa, localizados na parte superior da janela principal, a janela de navegação à esquerda, a janela de descrição à direita, no meio, e a janela de detalhes à direita, na parte inferior da janela principal.

5.4.1.1 Controles do programa

Esta seção contém a descrição de todos os controles do programa disponíveis no ESET SysInspector.

Arquivo
Clicando aqui, você pode armazenar o status do relatório atual para investigação posterior ou abrir um relatório armazenado anteriormente. Se desejar publicar o seu relatório, recomendamos que gere um relatório adequado para envio. Dessa forma, o relatório omite as informações confidenciais.

Observação: *Você pode abrir os relatórios do ESET SysInspector armazenados anteriormente simplesmente arrastando e soltando-os na janela principal.*

Árvore
Permite expandir ou fechar todos os nós

Lista
Contém funções para uma navegação mais fácil dentro do programa e diversas outras funções, como, por exemplo, encontrar informações online.

Importante: *Os itens destacados em vermelho são desconhecidos, por isso o programa os marca como potencialmente perigosos. Se um item estiver em vermelho, isso não significa automaticamente que você pode excluir o arquivo. Antes de excluir, verifique se os arquivos são realmente perigosos ou desnecessários.*

Ajuda
Contém informações sobre o aplicativo e as funções dele.

Detalhe
Influencia informações exibidas em outras seções da janela principal e, por essa razão, simplifica o uso do programa. No modo "Básico", você terá acesso a informações utilizadas para encontrar soluções para problemas comuns em seu sistema. No modo "Médio", o programa exibe detalhes menos usados; enquanto, no modo "Completo", o ESET SysInspector exibe todas as informações necessárias para solucionar problemas muito específicos.

Filtragem de itens
A filtragem de itens é mais adequada para encontrar arquivos suspeitos ou registrar entradas no sistema. Ajustando o controle deslizante, você pode filtrar itens pelo nível de risco deles. Se o controle deslizante estiver configurado mais à esquerda (Nível de risco 1), todos os itens serão exibidos. Se você mover o controle deslizante para a direita, o programa filtrará todos os itens menos perigosos que o nível de risco atual e exibirá apenas os itens que são mais suspeitos do que o nível exibido. Com o controle deslizante mais à direita, o programa exibirá apenas os itens perigosos conhecidos.

Todos os itens que pertencem ao intervalo de risco de 6 a 9 representam risco de segurança. Se você não estiver utilizando algumas das soluções de segurança da ESET, recomendamos que rastreie o seu sistema com o ESET Online Scanner depois que o programa encontrar esse item. O ESET Online Scanner é um serviço gratuito e pode ser encontrado em http://www.eset.eu/online-scanner.

Observação: *O nível de risco de um item pode ser rapidamente determinado comparando a cor do item com a cor no controle deslizante Nível de risco.*

Pesquisar
A opção Pesquisar pode ser utilizada para encontrar um item específico pelo nome ou por parte do nome. Os resultados da solicitação da pesquisa são exibidos na janela Descrição.

Retornar
Clicando na seta para trás e para a frente, você pode retornar às informações exibidas anteriormente na janela Descrição.

Seção do status
Exibe o nó atual na janela Navegação.

5.4.1.2 Navegação no ESET SysInspector

O ESET SysInspector divide vários tipos de informações em diversas seções básicas chamadas nós. Se disponíveis, você pode encontrar detalhes adicionais expandindo cada nó em seus subnós. Para abrir ou recolher um nó, apenas clique duas vezes no nome do nó ou então clique em ⊞ ou em ⊟, ao lado do nome do nó. À medida que percorrer a estrutura em árvore dos nós e subnós na janela Navegação, você pode encontrar vários detalhes para cada nó mostrado na janela Descrição. Se você percorrer itens da janela Descrição, detalhes adicionais de cada item podem ser exibidos na janela Detalhes.

A seguir, estão as descrições dos nós principais da janela Navegação e as informações relacionadas das janelas Descrição e Detalhes.

Executando processos
Esse nó contém informações sobre aplicativos e processos em execução no momento da geração do relatório. Na janela Descrição, você pode encontrar detalhes adicionais para cada processo, como, por exemplo, bibliotecas dinâmicas utilizadas pelo processo e a localização delas no sistema, o nome do fornecedor do aplicativo, o nível de risco do arquivo, etc.

A janela Detalhes contém informações adicionais para itens selecionados na janela Descrição, como o tamanho do arquivo ou seu hash.

Observação: *Um sistema operacional consiste em diversos componentes kernel importantes que são executados 24 horas por dia, 7 dias por semana e que fornecem funções básicas e vitais para outros aplicativos do usuário. Em alguns casos, tais processos são exibidos na ferramenta ESET SysInspector com o caminho do arquivo começando com \??\. Esses símbolos fornecem otimização de pré-início desses processos; eles são seguros para o sistema e, por essa razão, estão corretos.*

Seção do status
A janela Descrição contém uma lista de processos e aplicativos que se comunicam pela rede utilizando o protocolo selecionado na janela Navegação (TCP ou UDP), junto com os endereços remotos aos quais o aplicativo está conectado. Também é possível verificar o DNS que atribui endereços IP designados.

A janela Detalhes contém informações adicionais para itens selecionados na janela Descrição, como o tamanho do arquivo ou seu hash.

Entradas de registro importantes
Contém uma lista de entradas de registro selecionadas que estão relacionadas frequentemente a diversos problemas com o sistema, como aqueles que especificam os programas de inicialização, objetos auxiliares do navegador (BHO), etc.

Na janela Descrição, você pode descobrir quais arquivos estão relacionados a entradas de registro específicas. Você pode consultar detalhes adicionais na janela Detalhes.

Serviços
A janela Descrição contém uma lista de arquivos registrados como Serviços do Windows. É possível verificar a maneira como o serviço é configurado para iniciar, junto com detalhes específicos do arquivo na janela Detalhes.

Drivers
Uma lista de drivers instalados no sistema.

Arquivos críticos
A janela Descrição exibe o conteúdo dos arquivos críticos relacionados ao sistema operacional Microsoft Windows ®.

Informações do sistema
Contém informações detalhadas sobre hardware e software, junto com informações sobre as variáveis ambientais e os direitos do usuário configurados.

Detalhes do arquivo
Uma lista de arquivos de sistema importantes e arquivos da pasta Arquivos de programas. Informações adicionais específicas dos arquivos podem ser encontradas nas janelas Descrição e Detalhes.

Sobre
Informações sobre o ESET SysInspector

5.4.1.3 Comparar

O recurso Comparar permite que o usuário compare dois relatórios existentes. O resultado desse recurso é um conjunto de itens não comuns nos dois relatórios. Ele é adequado se você deseja manter controle das alterações no sistema – você pode, por exemplo, detectar a atividade de código malicioso.

Depois de ser iniciado, o aplicativo cria um novo relatório, que é exibido em uma nova janela. Navegue até **Arquivo** -> **Salvar relatório** para salvar um relatório em um arquivo. Os relatórios podem ser abertos e visualizados posteriormente. Para abrir um relatório existente, utilize o menu **Arquivo** -> **Abrir relatório**. Na janela principal do programa, o ESET SysInspector sempre exibe um relatório de cada vez.

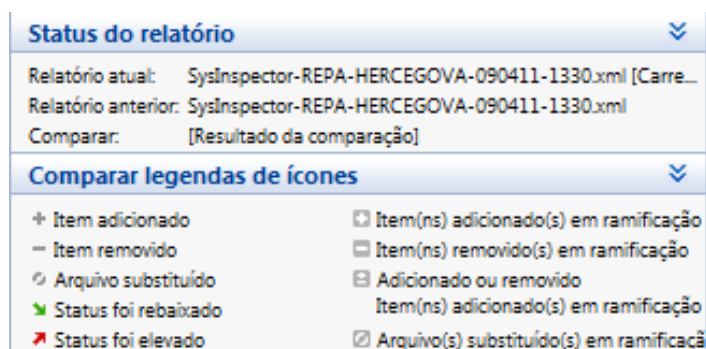
Se você comparar dois relatórios, o princípio reside no fato de você comparar um relatório ativo no momento com um relatório salvo em um arquivo. Para comparar relatórios, utilize a opção **Arquivo** -> **Comparar relatório** e escolha **Selecionar arquivo**. O relatório selecionado será comparado com o relatório ativo na janela principal do programa. O relatório resultante, chamado de relatório comparativo, exibirá apenas diferenças entre esses dois relatórios.

Observação: *Caso você compare dois relatórios, selecione Arquivo -> Salvar relatório e salve-o como um arquivo ZIP; os dois arquivos são salvos. Se você abrir tal arquivo posteriormente, os relatórios contidos serão comparados automaticamente.*

Ao lado dos itens exibidos, o SysInspector mostra os símbolos que identificam diferenças entre os relatórios comparados. Os itens marcados por um – podem ser encontrados apenas no relatório ativo e não estavam presentes no relatório comparativo aberto. Por outro lado, os itens marcados por um + estavam presentes apenas no relatório aberto e estavam ausentes no relatório ativo.

Descrição de todos os símbolos que podem ser exibidos ao lado dos itens:

- novo valor, ausente no relatório anterior
- a seção de estrutura em árvore contém novos valores
- valor removido, presente apenas no relatório anterior
- a seção de estrutura em árvore contém valores removidos
- o valor/arquivo foi alterado
- a seção de estrutura em árvore contém valores/arquivos modificados
- o nível de risco diminuiu / era maior no relatório anterior
- o nível de risco aumentou / era menor no relatório anterior

A seção de explicação exibida no canto inferior esquerdo descreve todos os símbolos e exibe também os nomes dos relatórios que estão sendo comparados.

Qualquer relatório comparativo pode ser salvo em um arquivo e aberto posteriormente.

Exemplo:
Gere e salve um relatório, registrando informações originais sobre o sistema, em um arquivo chamado previous.xml. Depois de terem sido feitas as alterações, abra o SysInspector e deixe-o gerar um novo relatório. Salve-o em um arquivo com o nome current.xml.

Para controlar as alterações entre esses dois relatórios, navegue até **Arquivo** -> **Comparar relatório**. O programa criará um relatório comparativo mostrando as diferenças entre eles.

O mesmo resultado poderá ser obtido se você utilizar a seguinte opção de linha de comando:

SysIsnpector.exe current.xml previous.xml

5.4.1.4 SysInspector como parte do ESET Smart Security 4

Para abrir a seção do SysInspector no ESET Smart Security 4 clique em **Ferramentas** > **SysInspector**. O sistema de gerenciamento da janela do SysInspector é semelhante ao sistema dos relatórios de rastreamento do computador ou das tarefas agendadas. Todas as operações com instantâneos do sistema: criar, visualizar, comparar, remover e exportar podem ser acessadas com um ou dois cliques.

A janela do SysInspector contém informações básicas sobre os instantâneos criados, como tempo de criação, breve comentário, nome do usuário que criou o instantâneo e o status do instantâneo.

Para **Comparar, Adicionar...** ou **Remover** instantâneos, utilize os botões correspondentes localizados abaixo da lista de instantâneos na janela do SysInspector. Essas opções estão disponíveis também no menu de contexto. Para exibir o instantâneo do sistema selecionado, utilize a opção do menu de contexto **Exibir**. Para exportar o instantâneo selecionado para um arquivo, clique com o botão direito do mouse e selecione **Exportar...**.A seguir, há uma descrição detalhada das opções disponíveis:

Comparar – permite comparar dois relatórios existentes. É adequada se você deseja controlar alterações entre o relatório atual e um relatório antigo. Para que essa opção seja efetivada, selecione dois instantâneos para serem comparados.

Adicionar – cria um novo registro. Antes disso, é preciso digitar um breve comentário sobre o registro. Para saber mais sobre o progresso de criação do instantâneo (do instantâneo gerado no momento) em porcentagem, consulte a coluna Status. Todos os instantâneos concluídos são marcados com o status Criado.

Remover – remove as entradas da lista

Mostrar – exibe o instantâneo selecionado. Ou então, é possível clicar duas vezes na entrada selecionada.

Exportar... – salva a entrada selecionada em um arquivo XML (também em uma versão compactada)

5.4.1.5 Script de serviços

O Script de serviços é uma ferramenta que influencia diretamente o sistema operacional e os aplicativos instalados, permitindo que os usuários executem scripts que removem os componentes problemáticos do sistema, incluindo vírus, restos de vírus, arquivos bloqueados, registros do vírus no registro etc. O script é armazenado em um arquivo de texto gerado a partir de um arquivo XML preexistente. Os dados no arquivo de script .txt são ordenados de maneira simples e legível para facilitar o uso. Inicialmente, o script apresentará um comportamento neutro. Em outras palavras, ele não terá nenhum impacto no sistema enquanto estiver na sua forma original. O usuário precisa editar o script para que ele tenha qualquer efeito.

Aviso:
Essa ferramenta é destinada apenas para usuários avançados. O uso incorreto pode resultar em dano a programas ou ao sistema operacional.

5.4.1.5.1 Geração de Scripts de serviços

Para gerar um script, clique com o botão direito do mouse em qualquer item da árvore de menus (no painel esquerdo) na janela principal do SysInspector. No menu de contexto, selecione a opção **Exportar todas as seções para script de serviços** ou a opção **Exportar as seções selecionadas para script de serviços**.

5.4.1.5.2 Estrutura do Script de serviços

Na primeira linha do cabeçalho do script, é possível encontrar informações sobre a Versão do mecanismo (ev), a Versão da GUI e a Versão do relatório (lv). Você pode usar esses dados para rastrear possíveis alterações no arquivo .xml que gera o script e evitar qualquer inconsistência durante a execução. Essa parte do script não deve ser alterada.

O restante do arquivo é dividido em seções em que os itens podem ser editados (indique aqueles que serão processados pelo script). Você marca os itens para processamento substituindo o caractere "-" na frente de um item por um caractere "+". As seções no script são separadas umas das outras por uma linha vazia. Cada seção tem um número e um título.

01) Processos em execução

Esta seção contém uma lista de todos os processos que estão em execução no sistema. Cada processo é identificado pelo seu caminho UNC e, posteriormente, pelo seu código hash CRC16 em asteriscos (*).

Exemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Nesse exemplo, um processo, o module32.exe, foi selecionado (marcado por um caractere "+"); o processo será finalizado após a execução do script.

02) Módulos carregados

Esta seção lista os módulos de sistema usados no momento.

Exemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll

- c:\windows\system32\advapi32.dll
[...]
```

Nesse exemplo, o módulo khbekhb.dll foi marcado por um "+". Quando o script for executado, ele reconhecerá os processos que utilizam esse módulo específico e os finalizará.

03) Conexões TCP

Esta seção contém informações sobre as conexões TCP existentes.

Exemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 ->
127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 ->
127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 ->
127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe
Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nas conexões TCP marcadas e interromperá o soquete, liberando recursos do sistema.

04) Pontos finais UDP

Esta seção contém informações sobre os pontos finais UDP existentes.

Exemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nos pontos finais UDP marcados e interromperá o soquete:

05) Entradas do servidor DNS

Esta seção contém informações sobre a configuração do servidor DNS atual.

Exemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

As entradas do servidor DNS marcadas serão removidas quando você executar o script.

06) Entradas importantes do registro

Esta seção contém informações sobre as entradas importantes do registro.

Exemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\
Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

As entradas marcadas serão excluídas, reduzidas a valores de 0 byte ou redefinidas para seus valores padrão após a execução do script. A ação a ser aplicada a uma entrada especial depende da categoria de entrada e do valor da chave no registro específico.

07) Serviços

Esta seção lista os serviços registrados dentro do sistema.

Exemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\
windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\
windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path:
c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

Os serviços marcados e seus serviços dependentes serão parados e desinstalados quando o script for executado.

08) Drivers

Esta seção lista os drivers instalados.

Exemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\
system32\drivers\acpi.sys, state: Running, startup:
Boot
- Name: ADI UAA Function Driver for High Definition
Audio Service, exe path: c:\windows\system32\drivers\
adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando você executar o script, os drivers selecionados terão seus registros cancelados no sistema e serão removidos.

09) Arquivos críticos

Esta seção contém informações sobre os arquivos críticos para o funcionamento adequado do sistema operacional.

Exemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]

* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]

* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Os itens selecionados serão excluídos ou redefinidos para seus valores originais.

5.4.1.5.3 Como executar Scripts de serviços

Marque todos os itens desejados, salve e feche o script. Execute o script editado diretamente da janela principal do SysInspector, selecionando a opção **Executar script de serviço** no menu Arquivo. Quando você abrir um script, o programa emitirá um aviso com a seguinte mensagem: **Tem certeza de que deseja executar o script de serviços "%Scriptname%"?** Depois de confirmar a sua seleção, outro aviso pode aparecer, informando que o script de serviços que você está tentando executar não foi assinado. Clique em **Executar** para iniciar o script.

Uma janela de diálogo confirmará a execução bem-sucedida do script.

Se o script puder ser processado apenas parcialmente, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços foi executado parcialmente. Deseja exibir o relatório de erros?** Selecione **Sim** para exibir um relatório complexo de erros, listando as operações que não foram executadas.

Seu script não foi reconhecido como válido e não será executado se você visualizar a seguinte mensagem: **Há algum problema com a consistência do script (título danificado, título da seção corrompido, faltando linha vazia entre seções etc.)?** Você pode reabrir o arquivo de script e corrigir os erros dentro do script ou criar um novo script de serviços.

5.5 ESET SysRescue

O CD de recuperação da ESET (ERCD) é um utilitário que possibilita criar um disco inicializável que contém o ESET Smart Security 4 (ESS). A principal vantagem do CD de recuperação da ESET é o fato de que o ESS é executado de maneira independente do sistema operacional host, ao mesmo tempo em que possui um acesso direto ao disco e a todo o sistema de arquivos. Graças a isso, é possível remover essas ameaças que normalmente não poderiam ser excluídas, por exemplo, quando o sistema operacional estiver em execução, etc.

5.5.1 Requisitos mínimos

O ESET SysRescue (ESR) funciona no Microsoft Windows Preinstallation Environment (Windows PE) versão 2.x, que é baseado no Windows Vista. O Windows PE faz parte do pacote grátis Windows Automated Installation Kit (Windows AIK), portanto o Windows AIK deve ser instalado antes da criação do ESR. Devido ao suporte da versão de 32 bits do Windows PE, o ESR pode ser criado apenas na versão de 32 bits do ESS/ENA. O ESR aceita o Windows AIK 1.1 e superior. O ESR está disponível no ESS/ENA 4.0 e superior.

5.5.2 Como criar o CD de restauração

Se os requisitos mínimos para a criação do CD do ESET SysRescue (ESR) forem atendidos, essa será uma tarefa bem fácil de executar. Para iniciar o assistente do ESR, clique em **Iniciar** > **Programas** > **ESET** > **ESET Smart Security 4** > **ESET SysRescue**.

Primeiro, o assistente verifica a presença do Windows AIK e de um dispositivo adequado para a criação da mídia de inicialização.

Na próxima etapa, selecione a mídia de destino em que o ESR estará localizado. Além do CD/DVD/USB, você pode optar por salvar o ESR em um arquivo ISO. Posteriormente, é possível gravar a imagem ISO em CD/DVD ou utilizá-la de alguma outra maneira (por exemplo, no ambiente virtual, como VmWare ou Virtualbox).

Após a especificação de todos os parâmetros, você terá uma visualização da compilação na última etapa do assistente do ESET SysRescue. Verifique os parâmetros e inicie a compilação. As opções disponíveis incluem:

Pastas
Antivírus da ESET
Avançado
Dispositivo USB inicializável
Gravação

5.5.2.1 Pastas

Pasta temporária é um diretório de trabalho para arquivos exigidos durante a compilação do ESET SysRescue.

Pasta ISO é uma pasta, em que o arquivo ISO resultante é salvo após a conclusão da compilação.

A lista nessa guia mostra todas as unidades de rede locais e mapeadas, junto com o espaço livre disponível. Se algumas dessas pastas estiverem localizadas em uma unidade com espaço livre insuficiente, recomendamos que você selecione outra unidade com mais espaço livre disponível. Caso contrário, a compilação pode ser encerrada prematuramente devido a espaço livre em disco insuficiente.

Aplicativos externos – Permite especificar programas adicionais que serão executados ou instalados após a inicialização de uma mídia do SysRescue.

Incluir aplicativos externos – permite adicionar programa externo à compilação do SysRescue.

Pasta selecionada – pasta em que os programas a serem adicionados ao disco do SysRescue estão localizados

5.5.2.2 Antivírus da ESET

Para a criação do CD do ESET SysRescue, é possível selecionar duas fontes de arquivos da ESET para serem utilizadas pelo compilador.

Pasta do ESS – arquivos já contidos na pasta na qual o produto da ESET está instalado no computador

Arquivo MSI – arquivos contidos no instalador do MSI são utilizados

Perfil – é possível utilizar uma das seguintes fontes de nome de usuário e senha:

ESS instalado – nome do usuário e senha são copiados do ESET Smart Security 4 ou do ESET NOD32 instalados atualmente

Do usuário – o nome de usuário e a senha digitados nas caixas de texto correspondentes abaixo são utilizados

Observação: *O ESET Smart Security 4 ou Antivírus ESET NOD32 presente no CD do ESET SysRescue é atualizado na Internet ou na solução de segurança da ESET instalada no computador em que o CD do ESET SysRescue está em execução.*

5.5.2.3 Avançado

A guia **Avançado** permite otimizar o CD do ESET SysRescue para o tamanho da memória do computador. Selecione **512 MB ou mais** para gravar o conteúdo do CD na memória operacional (RAM). Se você selecionar **menos de 512 MB**, o CD de recuperação será permanentemente acessado quando o WinPE estiver em execução.

Drivers externos – nesta seção, é possível inserir drivers para o seu hardware específico (geralmente adaptador de rede). Embora o WinPE seja baseado em Windows Vista SP1, que aceita hardware de larga escala, algumas vezes o hardware não é reconhecido e você precisa adicionar o driver manualmente. Há duas maneiras de inserir o driver na compilação do ESET SysRescue: manualmente (botão **Adicionar**) e automaticamente (botão **Pesquisa automática**). No caso de inserção manual, é preciso selecionar o caminho para o arquivo .inf correspondente (o arquivo *.sys aplicável também deve estar presente nessa pasta). Em caso de inserção automática, o driver é encontrado automaticamente no sistema operacional do computador especificado. Recomendamos utilizar a inserção automática apenas se o SysRescue for utilizado em um computador com o mesmo adaptador de rede como o utilizado no computador em que o SysRescue foi criado. Durante a criação do ESET SysRescue, o driver é inserido na compilação para que o usuário não precise procurá-lo separadamente mais tarde.

5.5.2.4 Dispositivo USB inicializável

Se você selecionou o dispositivo USB como mídia-alvo, é possível selecionar uma das mídias USB disponíveis na guia Dispositivo USB inicializável (caso haja mais dispositivos USB).

Aviso: *O dispositivo USB selecionado será formatado durante o processo de criação do ESET SysRescue, o que significa que todos os dados no dispositivos serão excluídos.*

5.5.2.5 Gravação

Se você selecionou CD/DVD como sua mídia-alvo, é possível especificar parâmetros de gravação adicionais na guia Gravar.

Excluir arquivo ISO – marque essa opção para excluir os arquivos ISO depois de criar o CD de restauração da ESET.

Exclusão ativada – permite selecionar o apagamento rápido e concluí-lo.

Dispositivo de gravação – selecione a unidade a ser utilizada para gravação.

Aviso: *Essa é a opção padrão. Se um CD/DVD regravável for utilizado, todos os dados contidos serão apagados.*

A seção Mídia contém informações sobre a mídia atual inserida em seu dispositivo de CD/DVD.

Velocidade de gravação – selecione a velocidade desejada no menu suspenso. Os recursos do seu dispositivo de gravação e o tipo de CD/DVD utilizado devem ser levados em consideração na seleção da velocidade de gravação.

5.5.3 Trabalho com o ESET SysRescue

Para usar o CD/DVD/USB de restauração de forma eficiente, é necessário que o computador seja inicializado a partir da mídia de inicialização do ESET SysRescue. A prioridade de inicialização pode ser modificada no BIOS. Ou então, você pode chamar o menu de inicialização durante a inicialização do computador, geralmente utilizando uma das teclas: F9 ou F12, dependendo da versão da placa-mãe/do BIOS.

Após a inicialização, o ESS/ENA será iniciado. Como o ESET SysRescue é utilizado apenas em situações específicas, alguns módulos de proteção e recursos de programa presentes no ESS/ENA regular não são necessários; a lista é limitada a Rastreamento do computador, Atualização e algumas seções na Configuração. A capacidade de atualização do banco de dados de assinatura de vírus é o recurso mais importante do ESET SysRescue. Recomendamos que você atualize o programa antes de iniciar um rastreamento do computador.

5.5.3.1 Uso do ESET SysRescue

Suponha que os computadores da rede tenham sido infectados por um vírus que modifica os arquivos executáveis (EXE). O ESS/ENA é capaz de limpar todos os arquivos infectados, exceto o explorer.exe, que não pode ser limpo, nem mesmo no Modo de segurança.

Isso é devido ao fato de que o explorer.exe, como um dos processos essenciais do Windows, é iniciado no Modo de segurança também. O ESS/ENA não pode executar nenhuma ação com o arquivo e portanto permanece infectado.

Em um cenário como esse, você pode empregar o ESET SysRescue para solucionar o problema. O ESET SysRescue não exige componentes do sistema operacional host. Portanto, ele pode processar (limpar, excluir) qualquer arquivo no disco.

6. Glossário

6.1 Tipos de ameaças

Uma ameaça é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

6.1.1 Vírus

Um vírus de computador é uma ameaça que corrompe os arquivos existentes em seu computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro.

Os vírus de computador atacam principalmente arquivos e documentos executáveis. Para se replicar, um vírus anexa seu "corpo" ao final de um arquivo de destino. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o vírus ativa a si próprio (antes do aplicativo original) e realiza sua tarefa predefinida. Somente depois disso, o aplicativo original pode ser executado. Um vírus não pode infectar um computador a menos que o usuário (acidental ou deliberadamente) execute ou abra ele mesmo o programa malicioso.

Os vírus de computador podem se ampliar em atividade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositalmente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

É importante observar que os vírus estão (quando comparados aos cavalos de Troia e aos spywares) gradualmente se tornando uma raridade, uma vez que eles não são comercialmente atrativos para os autores de softwares maliciosos. Além disso, o termo "vírus" é muitas vezes incorretamente usado para abranger todos os tipos de ameaças. No momento, isso está gradualmente sendo substituído e o novo termo "software malicioso", mais preciso, está sendo usado.

Se o seu computador estiver infectado por um vírus, será necessário restaurar os arquivos infectados para o seu estado original, ou seja, limpá-los usando um programa antivírus.

Os exemplos de vírus são: OneHalf, Tenga e Yankee Doodle.

6.1.2 Worms

Um worm de computador é um programa que contém código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se replicar e viajam por conta própria. Eles não dependem dos arquivos host (ou dos setores de inicialização).

Os worms se proliferam por email ou por pacotes da rede. Sob esse aspecto, os worms podem ser categorizados de dois modos:

- **Email** – distribuem-se para os endereços de email encontrados na lista de contatos do usuário e
- **Rede** – exploram as vulnerabilidades de segurança dos diversos aplicativos.

Os worms são portanto muito mais viáveis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o globo dentro de horas após sua liberação – em alguns casos, até em minutos. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos do que outros tipos de softwares maliciosos, como os vírus.

Um worm ativado em um sistema pode causar inúmeras inconveniências: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar alguns programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de ameaças.

Se o seu computador estiver infectado por um worm de computador, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

Exemplos de worms bem conhecidos são: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

6.1.3 Cavalos de Troia

Historicamente, os cavalos de Troia dos computadores foram definidos como uma classe de ameaça que tenta se apresentar como programas úteis, enganando assim os usuários que os deixam ser executados. Mas é importante observar que isso era verdadeiro para os cavalos de Troia do passado; hoje, não há necessidade que eles se disfarcem. O seu único propósito é se infiltrar o mais facilmente possível e cumprir com seus objetivos maliciosos. O "cavalo de Troia" tornou-se um termo muito genérico para descrever qualquer ameaça que não se encaixe em uma classe específica de ameaça.

Uma vez que essa é uma categoria muito ampla, ela é geralmente dividida em muitas subcategorias. As mais amplamente conhecidas são:

- downloader – um programa malicioso com a capacidade de fazer o download de outras ameaças a partir da Internet.
- dropper – um tipo de cavalo de Troia criado para instalar outros tipos de softwares maliciosos em computadores comprometidos.
- backdoor – um aplicativo que se comunica com agressores remotos, permitindo que eles obtenham acesso ao sistema e assumam o controle dele.
- keylogger – (keystroke logger) – programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- dialer – dialers são programas criados para se conectar aos números com tarifa premium. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modems discados que não são mais usados regularmente.

Os cavalos de Troia geralmente tomam a forma de arquivos executáveis com extensão .exe. Se um arquivo em seu computador for detectado como um cavalo de Troia, é aconselhável excluí-lo, uma vez que ele quase sempre contém códigos maliciosos.

Os exemplos dos cavalos de Troia bem conhecidos são: NetBus, Trojandownloader.Small.ZL, Slapper

6.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo em que ocultam a sua presença. Os rootkits, depois de acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows. Por essa razão, é quase impossível detectá-los com as técnicas comuns.

Quando se trata de prevenção do rootkit, lembre-se de que há dois níveis de detecção:

1. Quando eles tentam acessar um sistema. Eles ainda não estão presentes e estão portanto inativos. A maioria dos sistemas antivírus é capaz de eliminar rootkits nesse nível (supondo-se que eles realmente detectem tais arquivos como estando infectados).
2. Quando eles estão ocultos para os testes usuais. Os usuários do sistema antivírus da ESET têm a vantagem da tecnologia Anti-Stealth, que é capaz também de detectar e eliminar os rootkits ativos.

6.1.5 Adware

Adware é uma abreviação para advertising-supported software (software suportado por propaganda). Os programas exibindo material de publicidade pertencem a essa categoria. Os aplicativos Adware geralmente abrem automaticamente uma nova janela pop-up contendo publicidade em um navegador da Internet ou mudam a homepage do mesmo. O Adware está geralmente vinculado a programas freeware, permitindo que os criadores de freeware cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso; os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware pode também realizar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa de instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente, você poderá cancelá-lo e instalar o programa sem o adware. Por outro lado, alguns programas não serão instalados sem o adware ou as suas funcionalidades serão limitadas. Isso significa que o adware poderá acessar com frequência o sistema de modo "legal", pois os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar.

Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há uma grande probabilidade de ele conter códigos maliciosos.

6.1.6 Spyware

Essa categoria abrange todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Eles usam as funções de rastreamento para enviar diversos dados estatísticos como listas de sites visitados, endereços de email da lista de contato do usuário ou uma lista de teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e interesses dos usuários e permitir publicidade melhor direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINS, números de contas bancárias, etc. O Spyware geralmente está vinculado a versões gratuitas de um programa pelo seu autor, a fim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos clientes de redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica – eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável excluí-lo, uma vez que há uma grande possibilidade de ele conter códigos maliciosos.

6.1.7 Aplicativos potencialmente inseguros

Há muitos programas legítimos que servem para simplificar a administração de computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. Essa é a razão pela qual a ESET criou essa categoria especial. Nossos clientes têm agora a opção de escolher se o sistema antivírus deve ou não detectar tais ameaças.

"Aplicativos potencialmente inseguros" é a classificação usada para softwares comerciais, legítimos. Essa classificação inclui os programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que grava cada toque nas teclas digitadas pelo usuário).

Se você achar que há um aplicativo não seguro em potencial presente e sendo executado em seu computador (e que você não o instalou), consulte o seu administrador de rede ou remover o aplicativo.

6.1.8 Aplicativos potencialmente indesejados

Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo. Tais aplicativos geralmente exigem consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de forma diferente (em comparação ao estado antes da instalação). As alterações mais significativas são:

- são abertas novas janelas que você não via anteriormente
- ativação e execução de processos ocultos
- aumento no uso de recursos do sistema
- alterações nos resultados de pesquisa
- o aplicativo se comunica com servidores remotos

6.2 Tipos de ataques remotos

Há muitas técnicas especiais que permitem que os agressores comprometam os sistemas remotos. Elas são divididas em diversas categorias.

6.2.1 Ataques DoS

DoS, ou negação de serviço, é uma tentativa de tornar um computador ou rede indisponível para os seus usuários. A comunicação entre os usuários afetados é obstruída e não pode mais continuar de modo funcional. Os computadores expostos aos ataques DoS geralmente precisam ser reiniciados para que funcionem adequadamente.

Na maioria dos casos, os alvos são servidores web e o objetivo é torná-los indisponíveis aos usuários por um determinado período de tempo.

6.2.2 Envenenamento de DNS

Através do método de envenenamento de DNS (Domain Name Server), os hackers podem levar o servidor DNS de qualquer computador a acreditar que os dados falsos que eles forneceram são legítimos e autênticos. As informações falsas são então ocultadas por um determinado período de tempo, permitindo que os agressores reescrevam as respostas DNS dos endereços IP. Como resultado, os usuários que tentam acessar os sites da Internet farão o download de vírus ou worms em vez do seu conteúdo original.

6.2.3 Ataques de worms

Um worm de computador é um programa que contém código malicioso que ataca os computadores host e se espalha pela rede. Os worms da rede exploram as vulnerabilidades de segurança dos diversos aplicativos. Devido à disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de algumas horas após sua liberação. Em alguns casos, até mesmo em minutos.

A maioria dos ataques de worms (Sasser, SqlSlammer) pode ser evitada utilizando as configurações de segurança padrão no firewall ou bloqueando as portas não utilizadas e desprotegidas. Além disso, é essencial que o seu sistema operacional esteja atualizado com os patches de segurança mais recentes.

6.2.4 Rastreamento de portas

O rastreamento de portas verifica se há portas abertas do computador em um host da rede. Um rastreador de porta é um software desenvolvido para encontrar tais portas.

Uma porta de computador é um ponto virtual que lida com os dados de entrada e de saída e são cruciais do ponto de vista da segurança. Em uma rede grande, as informações reunidas pelos rastreadores de porta podem ajudar a identificar as vulnerabilidades em potencial. Tal uso é legítimo.

O rastreamento de porta é geralmente usado pelos hackers na tentativa de comprometer a segurança. Seu primeiro passo é enviar pacotes para cada porta. Dependendo do tipo de resposta, é possível determinar quais portas estão em uso. O rastreamento por si só não causa danos, mas esteja ciente de que essa atividade pode revelar as vulnerabilidades em potencial e permitir que os agressores assumam o controle remoto dos computadores.

Os administradores de rede são aconselhados a bloquear todas as portas não usadas e proteger as que estão em uso contra o acesso não autorizado.

6.2.5 Dessincronização TCP

A dessincronização TCP é uma técnica usada nos ataques do TCP Hijacking. Ela é acionada por um processo no qual o número sequencial dos pacotes recebidos diferem do número sequencial esperado. Os pacotes com um número sequencial inesperado são dispensados (ou salvos no armazenamento do buffer na janela de comunicação atual).

No estado de dessincronização, os dois pontos finais da comunicação dispensam os pacotes recebidos. Esse é o ponto em que os agressores remotos são capazes de se infiltrar e fornecer pacotes com um número sequencial correto. Os agressores podem até manipular a comunicação com os seus comandos ou modificá-la de alguma outra forma.

Os ataques TCP Hijacking têm por objetivo interromper as comunicações servidor-cliente ou peer-to-peer. Muitos ataques podem ser evitados usando autenticação para cada segmento TCP. Também é aconselhável usar as configurações recomendadas para os seus dispositivos de rede.

6.2.6 Relé SMB

O Relé SMB e o Relé SMB 2 são programas capazes de executar um ataque contra os computadores remotos. Os programas se aproveitam do protocolo de compartilhamento do arquivo SMB (Server Message Block) que é embutido no NetBios. Se um usuário compartilhar qualquer pasta ou diretório dentro da rede local, ele provavelmente usará esse protocolo de compartilhamento de arquivo.

Dentro da comunicação de rede local, as criptografias da senha são alteradas.

O Relé SMB recebe uma conexão nas portas UDP 139 e 445, detecta os pacotes trocados pelo cliente e o servidor e os modifica. Depois de conectar e autenticar, o cliente é desconectado. O Relé SMB cria um novo endereço de IP virtual. O novo endereço pode ser acessado usando o comando "net use \\192.168.1.1". O endereço pode então ser usado por qualquer uma das funções de rede do Windows. O Relé SMB detecta a comunicação do protocolo SMB, exceto para negociação e autenticação. Os agressores remotos podem usar o endereço IP enquanto o computador cliente estiver conectado.

O Relé SMB 2 funciona com o mesmo princípio do Relé SMB, exceto que ele usa os nomes do NetBIOS em vez dos endereços IP. Os dois executam ataques "man-in-the-middle". Esses ataques permitem que os agressores remotos leiam, insiram e modifiquem as mensagens trocadas entre dois pontos finais de comunicação sem serem notados. Os computadores expostos a tais ataques geralmente param de responder ou reiniciam inesperadamente.

Para evitar ataques, recomendamos que você use senhas ou chaves de autenticação.

6.2.7 Ataques ICMP

O ICMP (Protocolo de Controle de Mensagens da Internet) é um protocolo de Internet popular e amplamente utilizado. Ele é utilizado primeiramente por computadores em rede para enviar várias mensagens de erro.

Os atacantes remotos tentam explorar a fraqueza do protocolo ICMP. O protocolo ICMP é destinado à comunicação unidirecional que não exige qualquer autenticação. Isso permite que os atacantes remotos disparem ataques chamados de DoS (negação de serviço) ou ataques que dão acesso a pessoas não autorizadas aos pacotes de entrada e de saída.

Exemplos típicos de um ataque ICMP são ping flood, flood de ICMP_ECHO e ataques de smurfs. Os computadores expostos ao ataque ICMP são significativamente mais lentos (isso se aplica a todos os aplicativos que utilizam a Internet) e têm problemas para se conectar à Internet.

6.3 Email

Email ou correio eletrônico é uma forma moderna de comunicação e traz muitas vantagens. É flexível, rápido e direto. O email teve um papel crucial na proliferação da Internet no início dos anos 90.

Infelizmente, com seus altos níveis de anonimato, o email e a Internet abrem espaço para atividades ilegais, como, por exemplo, spams. Em uma classificação mais ampla, spam inclui propagandas não solicitadas, hoaxes e proliferação de software malicioso – códigos maliciosos. A inconveniência e o perigo para o usuário são aumentados pelo fato de que os custos de envio são próximos de zero, e os autores de spam possuem muitas ferramentas e recursos disponíveis para obter novos emails. Além disso, o volume e a variedade de spams dificultam muito o controle. Quanto mais você utiliza o seu email, maior é a possibilidade de acabar em um banco de dados de mecanismo de spam. Algumas dicas de prevenção:

- Se possível, não publique seu email na Internet
- Forneça seu email apenas a pessoas confiáveis
- Se possível, não use alias comuns; com alias mais complicados, a probabilidade de rastreamento é menor
- Não responda a spam que já chegou em sua caixa de entrada
- Tenha cuidado ao preencher formulários da Internet; esteja especialmente ciente de caixas de seleção, como "Sim, eu desejo receber informações sobre... na minha caixa de entrada"
- Utilize emails "especializados" – por exemplo, um para o trabalho, um para comunicação com amigos, etc.
- De vez em quando, altere o seu endereço de email
- Utilize uma solução antispam

6.3.1 Propagandas

A propaganda na Internet é uma das formas de publicidade que mais cresce. A propaganda por email usa este meio de comunicação como forma de contato. As suas principais vantagens de marketing são custo zero, alto nível de objetividade e eficácia, e o mais importante, as mensagens são enviadas quase imediatamente. Muitas empresas usam as ferramentas de marketing por email para ser comunicar de forma eficaz com os seus clientes atuais e prospectivos.

Esse meio de publicidade é legítimo, desde que o usuário esteja interessado em receber informações comerciais sobre alguns produtos. Mas o fato é que muitas empresas enviam mensagens comerciais em bloco não solicitadas. Nesses casos, a publicidade por email ultrapassa o razoável e se torna spam.

A quantidade de emails comerciais não solicitados se tornou um problema real, uma vez que não demonstra sinais de que vá diminuir. Os autores de emails não solicitados naturalmente tentam mascarar o spam como mensagens legítimas. Por outro lado, a grande quantidade de publicidade legítima pode causar reações negativas.

6.3.2 Hoaxes

Um hoax é a propagação de uma mensagem pela Internet. Geralmente é enviado por email e algumas vezes por ferramentas de comunicação, como ICQ e Skype. A própria mensagem é geralmente uma brincadeira ou uma lenda urbana.

Os hoaxes de vírus de computador tentar gerar FUD (medo, incerteza e dúvida) nos remetentes, levando-os a acreditar que há um "vírus desconhecido" excluindo arquivos e recuperando senhas ou executando alguma outra atividade perigosa em seu sistema.

Alguns hoaxes têm a intenção de causar constrangimento emocional. Os remetentes são geralmente solicitados a encaminhar essas mensagens para todos os seus contatos, o que aumenta o ciclo de vida do hoax. Há hoaxes de celular, pedidos de ajuda, pessoas oferecendo para enviar-lhe dinheiro do exterior, etc. Na maioria dos casos, é impossível identificar a intenção do criador.

A princípio, se você vir uma mensagem solicitando que você a encaminhe para todos os contatos que você conheça, ela pode ser muito bem um hoax. Há muitos sites especializados na Internet que podem verificar se o email é legítimo ou não. Antes de encaminhar, execute uma pesquisa na Internet sobre a mensagem que você suspeita que seja um hoax.

6.3.3 Roubo de identidade

O termo roubo de identidade define uma atividade criminal que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Seu objetivo é obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN, etc.

O acesso geralmente é feito pelo envio de um email passando-se por uma pessoa ou negócio confiável (instituição financeira, companhia de seguros). O email parecerá muito legítimo e conterá gráficos e conteúdo que podem vir originalmente da fonte pela qual ele está tentando se passar. Será solicitado que você digite, sob várias pretensões (verificação dos dados, operações financeiras) alguns de seus dados pessoais – números de contas bancárias ou nomes de usuário e senhas. Todos esses dados, se enviados, podem ser facilmente roubados ou usados de forma indevida.

Deve-se observar que os bancos, empresas de seguros e outras empresas legítimas nunca solicitarão nomes de usuário e senhas em um email não solicitado.

6.3.4 Reconhecimento de fraudes em spam

Geralmente, há poucos indicadores que podem ajudar a identificar spam (emails não solicitados) em sua caixa de correio. Se uma mensagem atender a pelo menos alguns dos critérios a seguir, muito provavelmente é uma mensagem de spam.

- o endereço do remetente não pertence a alguém de sua lista de contatos
- você recebe uma oferta de grande soma de dinheiro, mas tem de fornecer primeiro uma pequena soma
- você é solicitado a inserir, sob vários pretextos (verificação de dados, operações financeiras), alguns de seus dados pessoais: números de contas bancárias, nomes de usuário e senhas, etc.
- está escrito em um idioma estrangeiro
- você é solicitado a comprar um produto no qual você não tem interesse. Se decidir comprar de qualquer maneira, verifique se o remetente da mensagem é um fornecedor confiável (consulte o fabricante do produto original)
- algumas das palavras estão com erros de ortografia em uma tentativa de enganar o seu filtro de spams. Por exemplo "vaigra", em vez de "viagra", etc.

6.3.4.1 Regras

No contexto das soluções Antispam e dos clientes de email, as regras são as ferramentas para manipular as funções do email. Elas são constituídas de duas partes lógicas:

1. condição (por exemplo, uma mensagem recebida de um determinado endereço)
2. ação (por exemplo, a exclusão da mensagem, movendo-a para uma pasta especificada).

O número e a combinação de diversas regras com a solução Antispam. Essas regras servem como medidas contra spam (email não solicitado). Exemplos típicos:

- 1. condição: Uma mensagem recebida contém algumas palavras geralmente vistas nas mensagens de spam
2. ação: Excluir a mensagem
- 1. condição: Uma mensagem recebida contém um anexo com a extensão .exe
2. ação: Excluir o anexo e enviar a mensagem para a caixa de correio
- 1. condição: Uma mensagem que chega do seu patrão
2. ação: Mover a mensagem para a pasta "Trabalho".

Recomendamos que você use uma combinação de regras nos programas Antispam, a fim de facilitar a administração e filtrar com mais eficiência o spam (email não solicitado).

6.3.4.2 Filtro Bayesian

A filtragem de spam Bayesian é uma forma muito eficiente de filtragem de email usada por quase todos os produtos antispam. Ela é capaz de identificar os emails não solicitados com um alto grau de precisão. O filtro Bayesian pode funcionar de acordo com a determinação do usuário.

A funcionalidade baseia-se no seguinte princípio: O processo de aprendizagem acontece na primeira fase. O usuário marca manualmente um número suficiente de mensagens como mensagens legítimas ou spam (normalmente 200/200). O filtro analisa ambas as categorias e aprende, por exemplo, que o spam geralmente contém palavras como "rolex" ou "viagra", enquanto mensagens legítimas são enviadas pelos membros da família ou dos endereços na lista de contato do usuário. Desde que um número maior de mensagens seja processado, o filtro Bayesian é capaz de atribuir determinado "índice de spam" para cada mensagem e assim decidir se é spam ou não.

A principal vantagem é a sua flexibilidade. Se um usuário for, digamos, um biólogo, todas as mensagens de email referentes à biologia ou aos campos de estudo relacionados serão geralmente recebidas com um índice de baixa probabilidade. Se uma mensagem incluir palavras que, ao contrário, a qualificam como não solicitada, mas que foi enviada por alguém de uma lista de contatos, ela será marcada como legítima, porque os remetentes de uma lista de contatos diminuem a probabilidade geral de spam.

6.3.4.3 Lista de permissões

Em geral, uma lista de permissões é uma lista de itens ou pessoas que são aceitas, ou para os quais foi concedida permissão de acesso. O termo "lista de permissões de email" define uma lista de contatos de quem o usuário deseja receber mensagens. Tais listas de permissões são baseadas nas palavras-chave para os endereços de email, nomes de domínio, endereços IP.

Se uma lista de permissões funcionar de "modo exclusivo", então as mensagens de qualquer outro endereço, domínio ou endereço IP não serão recebidas. Por outro lado, se não forem exclusivas, tais mensagens não serão excluídas, mas filtradas de algum modo.

Uma lista de permissões baseia-se no princípio oposto de uma lista de proibições. As listas de permissões são relativamente fáceis de serem mantidas, mais do que as listas de proibições. Recomendamos que você use tanto a Lista de permissões como a Lista de proibições para filtrar os spams com mais eficiência.

6.3.4.4 Lista de proibições

Geralmente, uma lista de proibições é uma lista de itens ou pessoas proibidos ou inaceitáveis. No mundo virtual, é uma técnica que permite aceitar mensagens de todos os usuários não presentes em uma determinada lista.

Há dois tipos de lista de proibições. É possível para os usuários criar suas próprias listas de proibições nos seus programas Antispam. Por outro lado, muitas listas de proibições muito profissionais, criadas por instituições especializadas podem ser encontradas na Internet.

Uma Lista de proibições baseia-se no princípio oposto ao da Lista de permissões. É essencial usar as Listas de proibições para bloquear spam com êxito, mas é muito difícil mantê-las, uma vez que novos itens não bloqueados aparecem todos os dias. Recomendamos que você use tanto a Lista de permissões como a Lista de proibições para filtrar os spams com mais eficiência.

6.3.4.5 O controle pelo servidor

O controle pelo servidor é uma técnica para identificar os emails de spam em massa com base no número de mensagens recebidas e as reações dos usuários. Cada mensagem deixa um "rastro" digital único no servidor com base no conteúdo da mensagem. Na verdade, é um número de ID único que não diz nada sobre o conteúdo do email. Duas mensagens idênticas terão rastros idênticos, enquanto mensagens diferentes terão rastros diferentes.

Se uma mensagem for marcada como spam, seu rastro será enviado ao servidor. Se o servidor receber mais de um rastro idêntico (correspondendo a uma determinada mensagem de spam), o rastro será armazenado no banco de dados de rastros de spam. Ao verificar as mensagens de entrada, o programa envia os rastros das mensagens ao servidor. O servidor retorna as informações sobre que rastros correspondem às mensagens já marcadas pelos usuários como spam.